# Application Notes for Configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager to Support Remote Users with NAT Traversal - Issue 1.0

## Abstract

These Application Notes describes the procedures for configuring Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with both near-end and far-end network address translation (NAT) traversal.

Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describes the procedure for configuring Sipera IPCS 310 with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Sipera IPCS 310 is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network with both near-end and far-end network address translation (NAT) traversal.

## 1.1. Configuration

**Figure 1** illustrates the test configuration. The test configuration shows several remote users connected by different means to an untrusted IP network to access the SIP infrastructure at a main enterprise site. The main site has a Netscreen 50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise, as well as performing NAT. NAT is provided by mapping the internal host address to a static public WAN address for each server that needs to be accessed externally. This includes IPCS and the TFTP server. Port address translation is not being performed at the enterprise. IPCS connects to a separate port of the firewall representing the demilitarized zone (DMZ) of the enterprise. The firewall will allow incoming SIP and RTP traffic directed to IPCS and incoming TFTP traffic to the TFTP server. Outbound traffic will be unrestricted.

The remote SIP endpoints will register and direct SIP and RTP traffic to the public IP address of IPCS. IPCS in return will register and direct SIP and RTP traffic on behalf of these endpoints to Avaya SES. IPCS uses its private LAN IP address to communicate with Avaya SES. In this manner, IPCS can protect the main site infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams.

Located at the main site on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints include two Avaya 4600 Series IP Telephones (with SIP firmware), an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. One PSTN number assigned to the ISDN-PRI trunk at the main site is mapped to a telephone extension at the main site. The other is mapped to a telephone extension of one of the remote users.

The Avaya 4600 Series IP Telephones (with SIP firmware) located at the main site are registered to Avaya SES. All calls originating from Avaya Communication Manager at the main office and destined for the remote users will be routed through the on-site Avaya SES, IPCS, data firewall and across the untrusted IP network.

The remote users are comprised of the following:

- An Avaya 4600 Series IP Telephone (with SIP firmware) connected directly to the untrusted network.
- An Avaya 4600 Series IP Telephone (with SIP firmware) connected behind a Netscreen 5GT firewall.  This firewall is configured to perform both network address and port translation (NAPT).
- Two Avaya 4600 Series IP Telephones (with SIP firmware) connected behind a second Netscreen 5GT firewall.  This firewall is configured to perform both network address and port translation.

The remote users register with Avaya SES through IPCS.  These telephones use the public IP address of IPCS at the main office as their configured server.  IPCS will forward any registration messages it receives from the remote endpoints to Avaya SES.  All calls originating from the remote users are routed across the untrusted IP network, the enterprise data firewall, IPCS and Avaya SES to Avaya Communication Manager at the main site.

All SIP telephones, both local and remote, use the TFTP server at the main site to obtain their configuration files.  All non-SIP traffic (including these TFTP transfers) bypasses IPCS and flows directly between the untrusted network to the private LAN of the enterprise if permitted by the firewall.

For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**).  This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

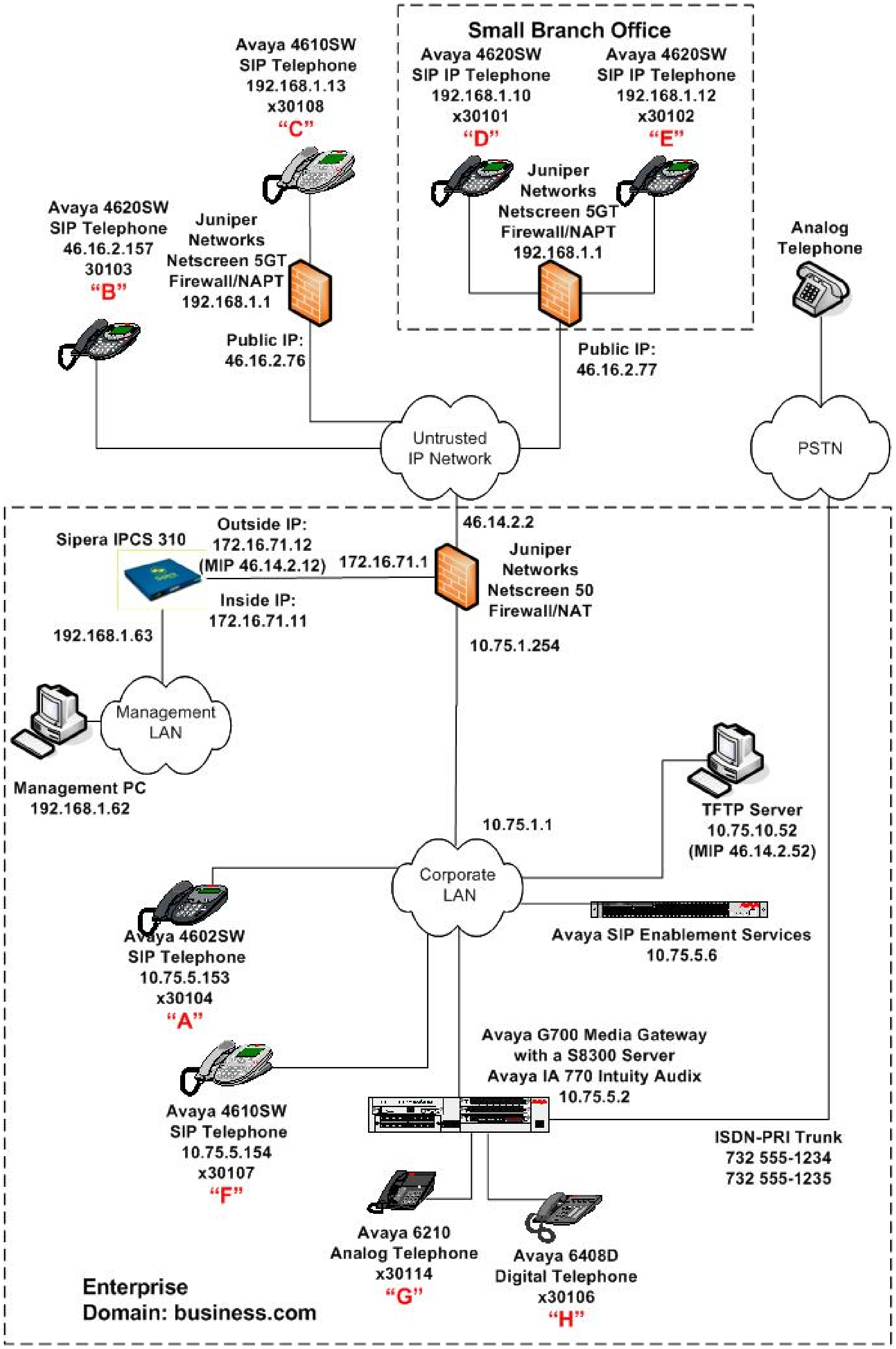


**Figure 1: IPCS 310 Test Configuration**

## 2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

| Equipment | Software/Firmware |
|---|---|
| Avaya S8300 Server with Avaya G700 Media Gateway<br>Avaya IA 770 Intuity Audix | Avaya Communication Manager 4.0 Service Pack (R014x.00.0.730.5-13566) |
| Avaya SIP Enablement Services (SES) | 3.1.2 |
| Avaya 4602SW IP Telephone<br>Avaya 4610SW IP Telephones<br>Avaya 4620SW IP Telephones | SIP version 2.2.2 |
| Avaya 6408D Digital Telephone | - |
| Avaya 6210 Analog Telephone | - |
| Analog Telephone | - |
| Windows PCs (Management PC and TFTP Server) | Windows XP Professional |
| Juniper Networks Netscreen 50 | 5.4.0r1.0 |
| Juniper Networks Netscreen 5GTs | 5.4.0r3a.0 |
| Sipera IPCS 310 | 3.1 (Build I51) |

## 3. Configure Avaya Communication Manager

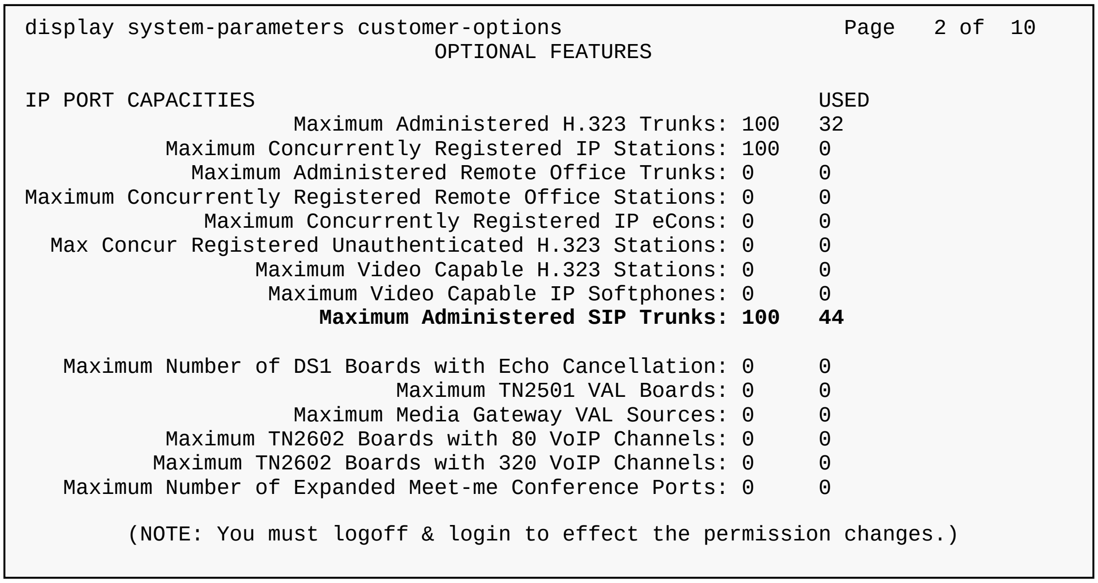
This section describes the Avaya Communication Manager configuration to support SIP and is typically comprised of two parts. The first part is the configuration of the SIP connection to Avaya SES required of any Avaya SES installation. The second part describes the configuration of Off-PBX stations (OPS) for each SIP endpoint. The configuration of the OPS stations is not directly related to the interoperability of IPCS, so it is not included here. The procedure for configuring OPS stations can be found in [4].

The following configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

Use the **display system-parameters customer-options** command to verify that sufficient SIP trunk capacity exists. On **Page 2**, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.

The license file installed on the system controls the maximum permitted. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.



```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   32
           Maximum Concurrently Registered IP Stations: 100   0
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 100   44

   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

</td></tr>
<tr><td>2.</td><td>

In order to support SIP the following features must be enabled. Use the **display system-parameters customer-options** command to verify that the following fields have been set to ***y***.

**Page 4**: **Enhanced EC500?** ***y***<br>
**Page 4**: **ISDN-PRI?** ***y***<br>
**Page 4**: **IP trunks?** ***y***

If a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

</td></tr>
</table>

| Step | Description |
|---|---|
| 3. | Use the **change node-names ip** command to assign the node name and IP address for Avaya SES. In this case, ***SES*** and ***10.75.5.6*** are being used, respectively. The node name ***SES*** will be used throughout the other configuration forms of Avaya Communication Manager. In this example, ***procr*** and ***10.75.5.2*** are the name and IP address assigned to the Avaya S8300 Server. |

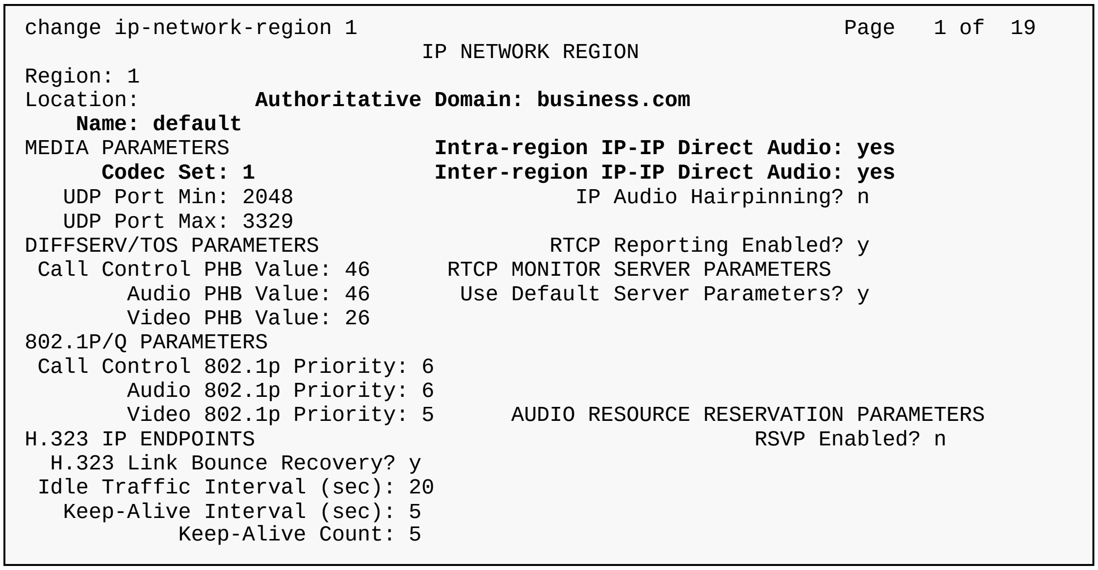
```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
SES                    10.75.5.6
default                0.0.0.0
myaudix                10.75.5.7
procr                  10.75.5.2
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

Use the **change ip-network-region *n*** command, where ***n*** is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. Select an IP network region that will contain the Avaya SES server. The association between this IP network region and the Avaya SES server will be done on the **Signaling Group** form as shown in **Step 6**. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Server and Avaya IP Telephones was selected to contain the Avaya SES server. By default, the Avaya S8300 Server and IP telephones are in IP network region 1.

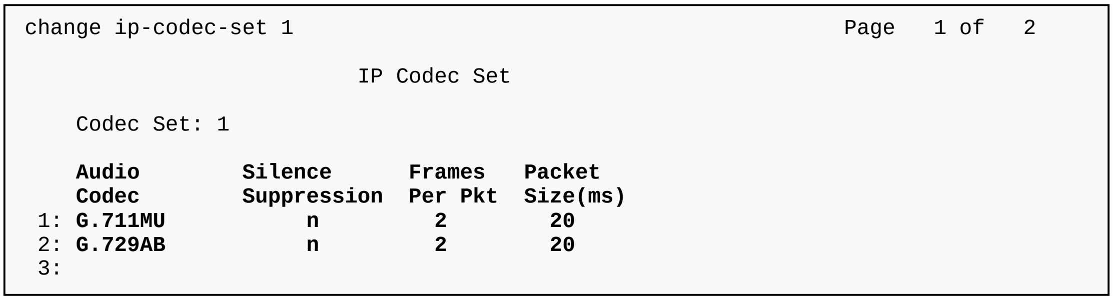
On the **IP Network Region** form:

- The **Authoritative Domain** field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***business.com***. This name will appear in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name for the **Name** field.
- By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G700 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used for the Avaya S8300 Server and the Avaya SES server, then **Page 3** of each **IP Network Region** form must be used to specify the codec set for inter-region communications.
- The default values can be used for all other fields.



```
change ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
Region: 1
Location:         Authoritative Domain: business.com
    Name: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

</td></tr>
</table>

| Step | Description |
|---|---|
| 5. | Use the **change ip-codec-set *n*** command, where ***n*** is the codec set value specified in **Step 4**, to enter the supported audio codecs. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test.<br> |

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729AB           n         2        20
 3:
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>

Use the **add signaling-group *n*** command, where ***n*** is the number of an unused signaling group, to create the SIP signaling group as follows:

- Set the **Group Type** field to ***sip***.
- The **Transport Method** field will default to ***tls*** (Transport Layer Security). TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager.
- Specify the Avaya S8300 Server (node name ***procr***) and the Avaya SES server (node name ***SES***) as the two ends of the signaling group in the **Near-end Node Name** and the **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Step 3**. For alternative configurations that use a C-LAN board, the near (local) end of the SIP signaling group will be the C-LAN board instead of the Avaya S8300 Server.
- Ensure that the TLS port value of ***5061*** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP network region value assigned in the **IP Network Region** form in **Step 4**. This defines which IP network region contains the Avaya SES server. If the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions.
- Enter the domain name of Avaya SES in the **Far-end Domain** field. In this configuration, the domain name is ***business.com***. This domain is specified in the Uniform Resource Identifier (URI) of the SIP "To" header in the INVITE message.
- The **Direct IP-IP Audio Connections** field is set to ***n***. For interoperability, this field (also know as media shuffling) must be disabled for the SIP trunk.
- The **DTMF over IP** field must be set to the default value of ***rtp-payload*** for a SIP trunk. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833.
- The default values for the other fields may be used.

```
add signaling-group 1                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
                       Transport Method: tls



   Near-end Node Name: procr               Far-end Node Name: SES
 Near-end Listen Port: 5061              Far-end Listen Port: 5061
                                      Far-end Network Region: 1
       Far-end Domain: business.com

                                           Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? n
                                                      IP Audio Hairpinning? n
 Enable Layer 3 Test? n
 Session Establishment Timer(min): 120
```

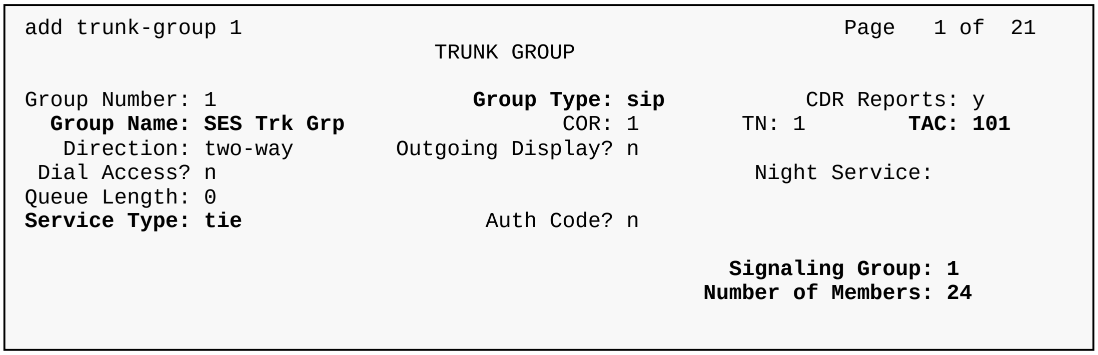
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

Add a SIP trunk group by using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen.

On **Page 1**, set the fields to the following values:

- Set the **Group Type** field to ***sip***.
- Choose a descriptive **Group Name**.
- Specify an available trunk access code (**TAC**) that is consistent with the existing dial plan.
- Set the **Service Type** field to ***tie***.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Step 6**.
- Specify the **Number of Members** supported by this SIP trunk group. As mentioned earlier, each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.
- The default values may be retained for the other fields.

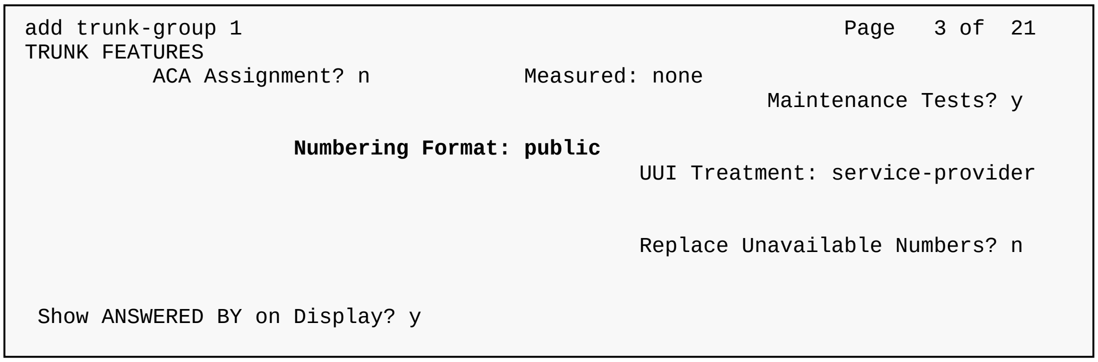


```
add trunk-group 1                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 1                  Group Type: sip           CDR Reports: y
  Group Name: SES Trk Grp               COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                        Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                    Signaling Group: 1
                                                  Number of Members: 24
```

</td></tr>
<tr><td>8.</td><td>

On **Page 3**:

- Verify the **Numbering Format** field is set to ***public***. This field specifies the format of the calling party number sent to the far-end.
- The default values may be retained for the other fields.



```
add trunk-group 1                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider


                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

</td></tr>
</table>

| Step | Description |
|---|---|
| 9. | Use the **change public-unknown-numbering 0** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in **Step 7**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 1 will be sent as a 5 digit calling number. This calling party number will be sent to the far-end in the SIP “From” header. |

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 4
 5  3             1                         5           Maximum Entries: 240
 5  3             99                        5
```

| Step | Description |
|---|---|
| 10. | Create a route pattern that will use the SIP trunk that connects to Avaya SES. This route pattern will be used as a default route for SIP calls in **Step 11**. Some transfer scenarios using alphanumeric handles (i.e., user names) instead of extensions require a default route pattern. These call scenarios were not tested as part of the compliance test, however, the creation of this default route pattern is included here for completeness.<br>To create a route pattern, use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values may be retained for all other fields. |

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 3   Pattern Name: SIP
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 3 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

**Step** | **Description**

11. Use the **change locations** command to assign the default SIP route pattern to the location. All IP endpoints, both local and remote, are part of a single logical location in Avaya Communication Manager with the default name of ***Main*** and shown in the example below. Enter the route pattern number from the previous step in the **Proxy Sel Rte Pat** field. The default values may be retained for all other fields.

```
change locations                                                Page   1 of   4
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name           Timezone Rule  NPA  ARS  Atd      Disp   Prefix   Proxy Sel
 No                   Offset             FAC  FAC      Parm              Rte Pat
 1:  Main            + 00:00   0                        1                  1
 2:                      :
 3:                      :
```

12. Automatic Route Selection (ARS) is used to route calls to the PSTN. In the compliance test, PSTN numbers that begin with 1732 were used for testing.

Use the **change ars analysis *n*** command to add an entry in the ARS Digit Analysis Table for the dialed string beginning with ***n***. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 2. Route pattern 2 routes calls to the ISDN-PRI trunk between the main site and the PSTN shown in **Figure 1**. The configuration of the PRI trunk is beyond the scope of these Application Notes.

```
change ars analysis 1732                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    3

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    1732                  11   11    2        fnpa          n
    174                   11   11    deny     fnpa          n
    175                   11   11    deny     fnpa          n
    176                   11   11    deny     fnpa          n
    177                   11   11    deny     fnpa          n
```

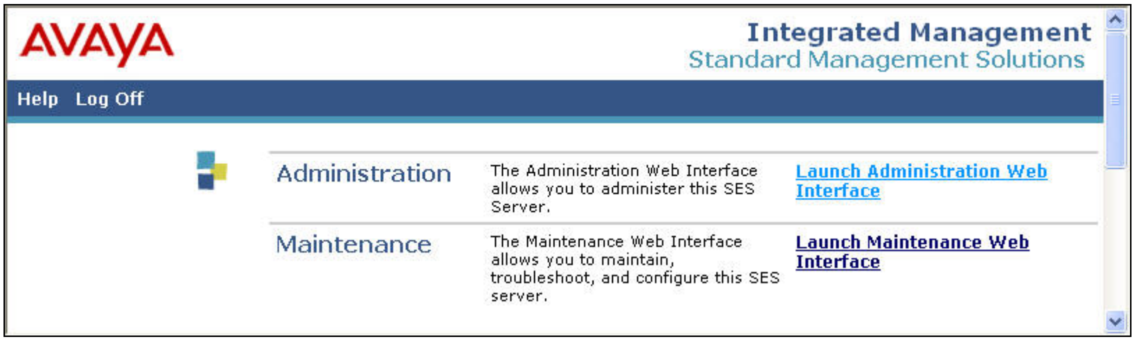
13. To map a PSTN number to a station at the main site or to a remote user, use the **change inc-call-handling-trmt trunk-group *n*** command, where ***n*** is the trunk group number connected to the PSTN from the Avaya G700 Media Gateway. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows two incoming 11-digit numbers being deleted and replaced with the extension number of the desired station.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Called    Called      Del Insert          Per Call Night
 Feature        Len      Number                          CPN/BN   Serv
 tie             11 17325551234      11  30104
 tie             11 17325551235      11  30101
```

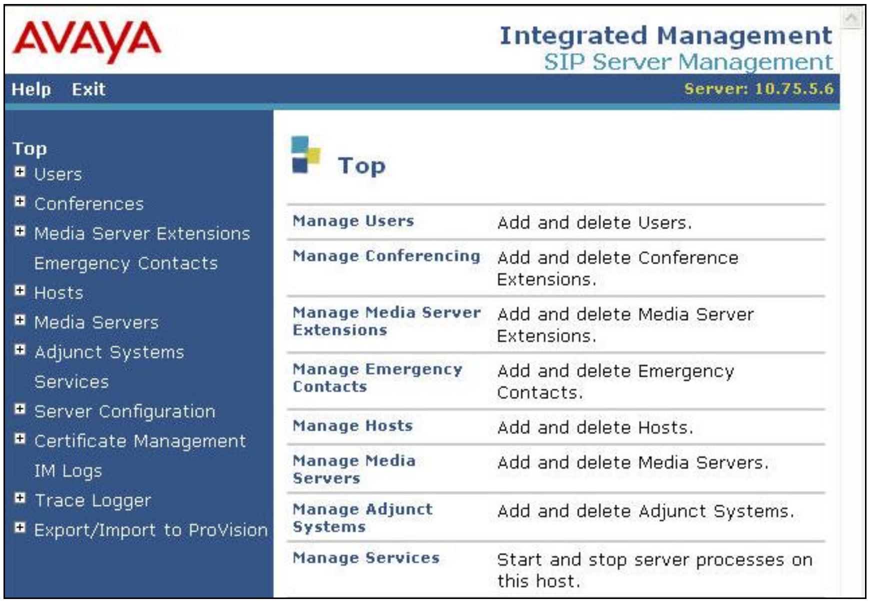
# 4. Configure Avaya SES

This section covers the configuration of Avaya SES. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the **Setup** screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].
2
Each SIP endpoint used in the compliance test, requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of IPCS so it is not included here. These procedures are covered in [5].

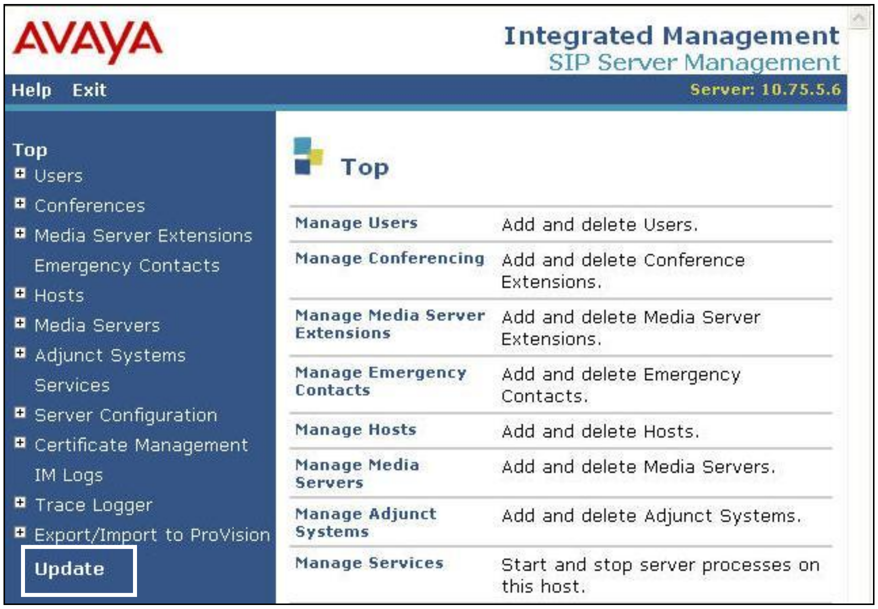
IPCS registers to Avaya SES on behalf of each of the remote users by serving as a proxy of the registration request from the remote endpoint to Avaya SES. Thus, IPCS appears as a set of endpoints to Avaya SES. As a result, no outbound proxy settings, address maps or trusted host settings are required on Avaya SES to route calls to or to support the remote users.

| Step | Description |
|---|---|
| 1. | Access the Avaya SES administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server.<br>Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown below.<br><br>Administration: The Administration Web Interface allows you to administer this SES Server. Launch Administration Web Interface<br>Maintenance: The Maintenance Web Interface allows you to maintain, troubleshoot, and configure this SES server. Launch Maintenance Web Interface<br> AVAYA<br>Integrated Management<br>Standard Management Solutions<br>Help<br>Log Off |

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>
The Avaya SES administration home page will be displayed as shown below.



<table>
<tr><td>Manage Users</td><td>Add and delete Users.</td></tr>
<tr><td>Manage Conferencing</td><td>Add and delete Conference Extensions.</td></tr>
<tr><td>Manage Media Server Extensions</td><td>Add and delete Media Server Extensions.</td></tr>
<tr><td>Manage Emergency Contacts</td><td>Add and delete Emergency Contacts.</td></tr>
<tr><td>Manage Hosts</td><td>Add and delete Hosts.</td></tr>
<tr><td>Manage Media Servers</td><td>Add and delete Media Servers.</td></tr>
<tr><td>Manage Adjunct Systems</td><td>Add and delete Adjunct Systems.</td></tr>
<tr><td>Manage Services</td><td>Start and stop server processes on this host.</td></tr>
</table>
</td></tr>
<tr><td>3.</td><td>
After making changes within Avaya SES, it is necessary to commit the database changes using the <b>Update</b> link that appears when changes are pending.  Perform this step by clicking on the <b>Update</b> link found in the bottom of the blue navigation bar on the left side of any of the Avaya SES administration pages as shown below.  It is recommended that this be done after making any changes.



<table>
<tr><td>Manage Users</td><td>Add and delete Users.</td></tr>
<tr><td>Manage Conferencing</td><td>Add and delete Conference Extensions.</td></tr>
<tr><td>Manage Media Server Extensions</td><td>Add and delete Media Server Extensions.</td></tr>
<tr><td>Manage Emergency Contacts</td><td>Add and delete Emergency Contacts.</td></tr>
<tr><td>Manage Hosts</td><td>Add and delete Hosts.</td></tr>
<tr><td>Manage Media Servers</td><td>Add and delete Media Servers.</td></tr>
<tr><td>Manage Adjunct Systems</td><td>Add and delete Adjunct Systems.</td></tr>
<tr><td>Manage Services</td><td>Start and stop server processes on this host.</td></tr>
</table>
</td></tr>
</table>

| Step | Description |
|---|---|
| 4. | As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each parameter is a brief description of how to view the value from the Avaya SES administration home page shown in the previous step.<br>• SIP Domain: ***business.com***<br>(To view, navigate to **Server Configuration→System Parameters**)<br>• Host (SES IP address): ***10.75.5.6***<br>(To view, navigate to **Host→List**; Click **Edit**)<br>• Media Server (Avaya Communication Manager) Interface Name: ***CMeast***<br>(To view, navigate to **Media Server→List**; Click **Edit**)<br>• SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2***<br>(To view, navigate to **Media Server→List**; Click **Edit**) |

## 5. Configure the Avaya SIP Telephones

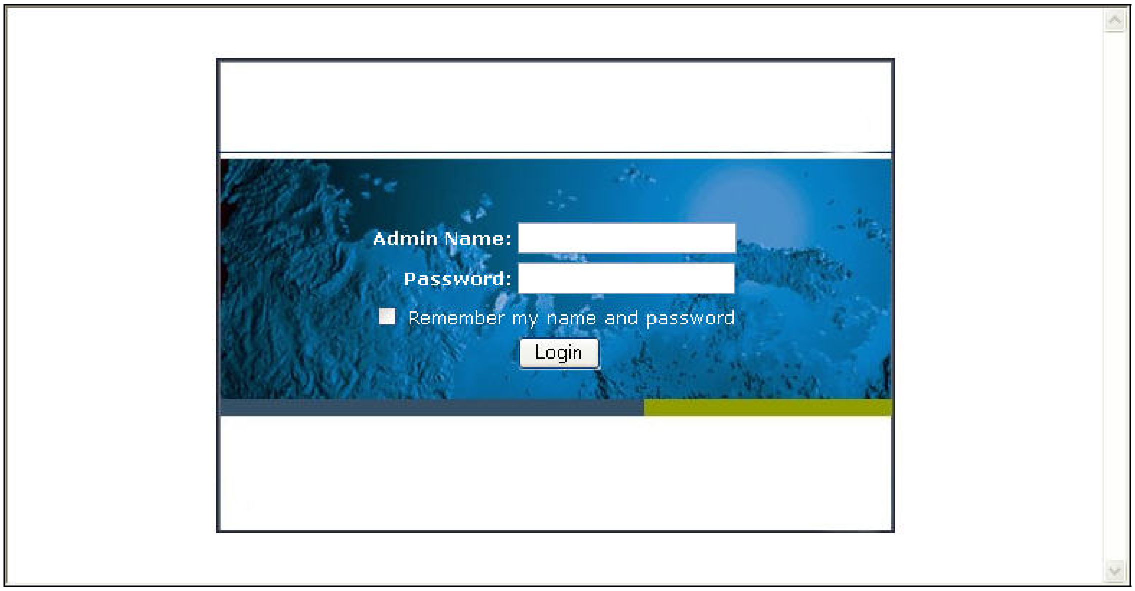
The SIP telephones at the main office will use Avaya SES as the call server. The SIP telephones of the remote users will use the mapped public IP address of IPCS as the call server.

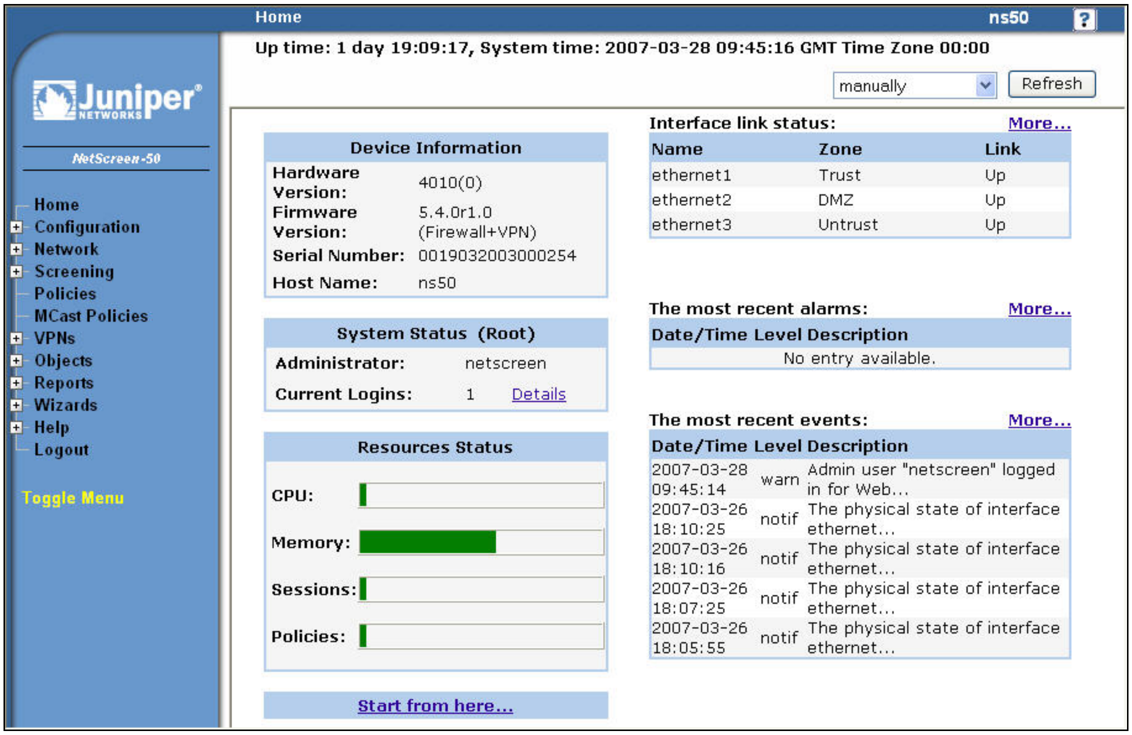
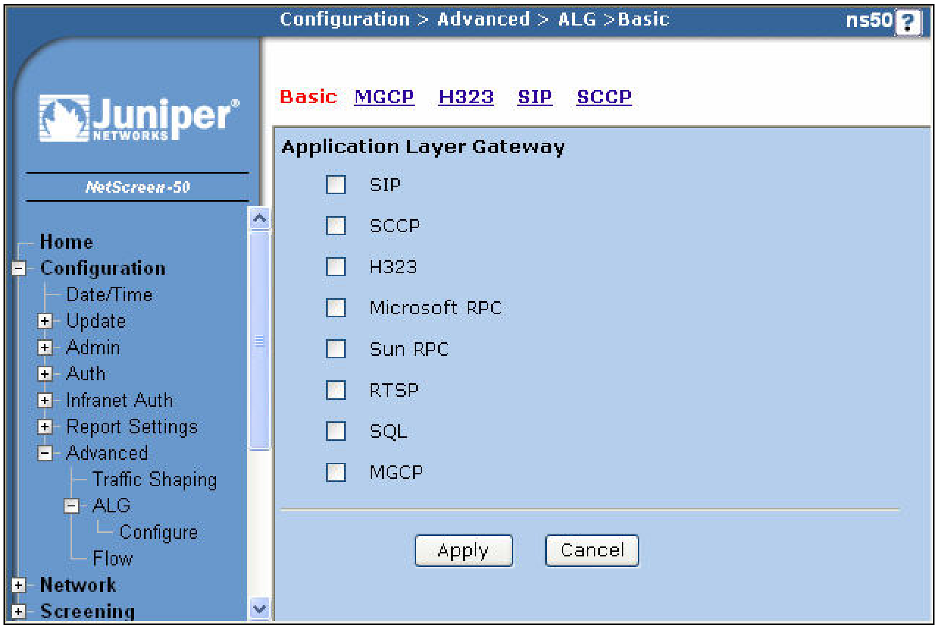
The table below shows an example of the SIP telephone networking settings for both the main site and remote.

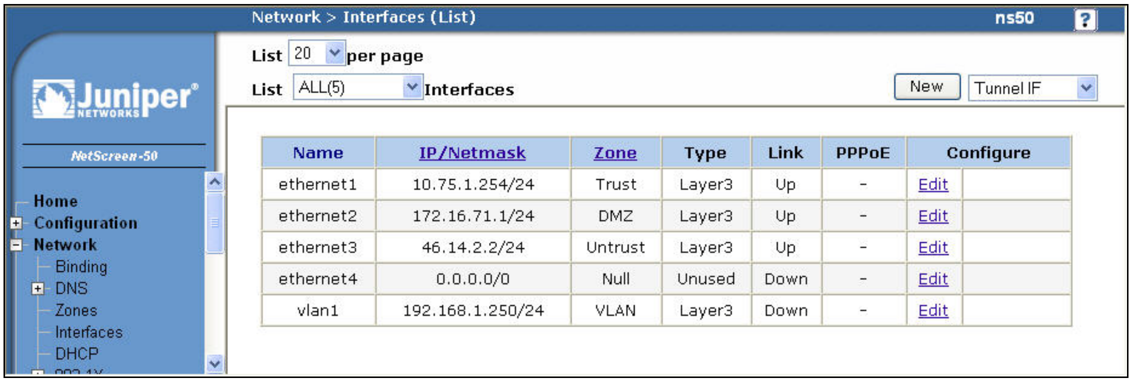
| | **Main Site** | **Remote User w/o NAT** | **Remote User w/ NAT** |
|---|---|---|---|
| IP Address | 10.75.5.153 | 46.16.2.157 | 192.168.1.10 |
| Subnet Mask | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| Call Server | 10.75.5.6 | 46.14.2.12 | 46.14.2.12 |
| Router | 10.75.5.1 | 46.16.2.1 | 192.168.1.1 |
| File Server | 10.75.10.52 | 46.14.2.52 | 46.14.2.52 |

# 6. Configure Juniper Networks Netscreen 50

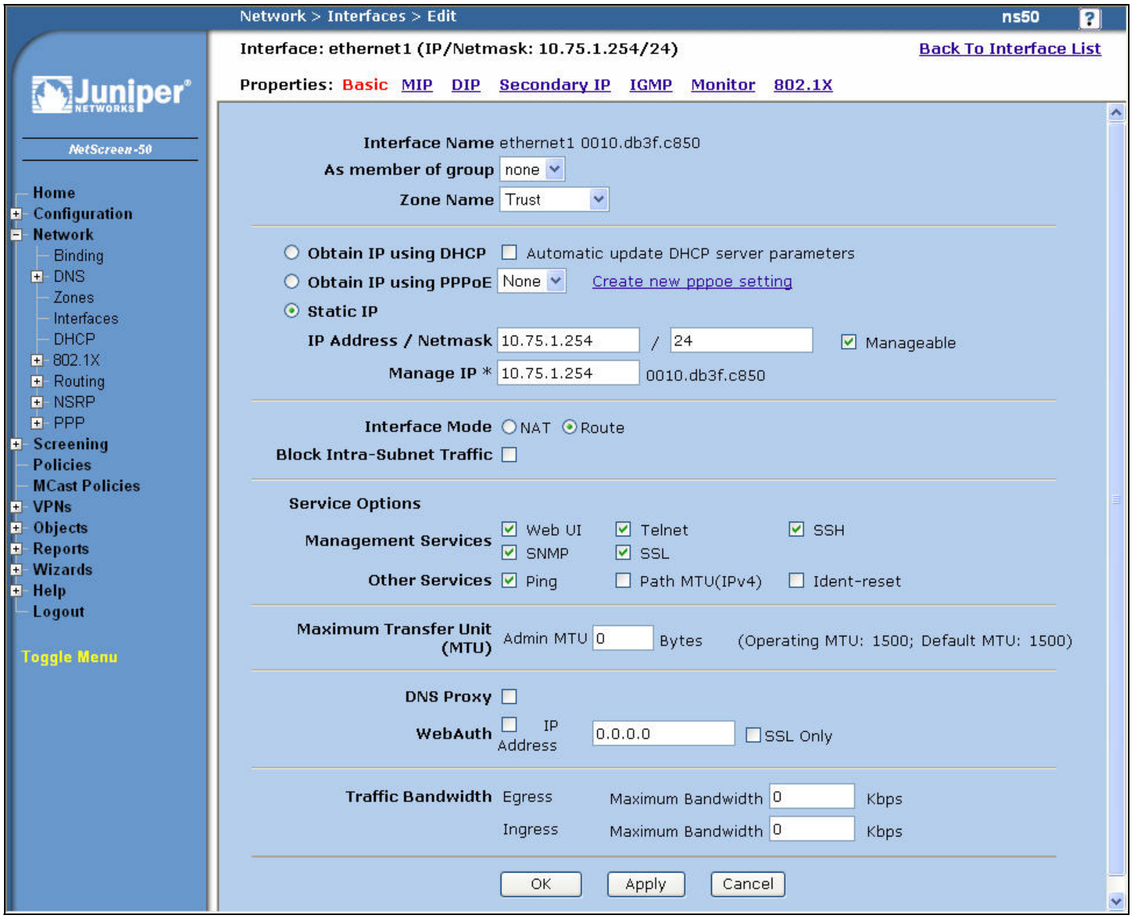
This section covers the configuration of the Netscreen 50 firewall.

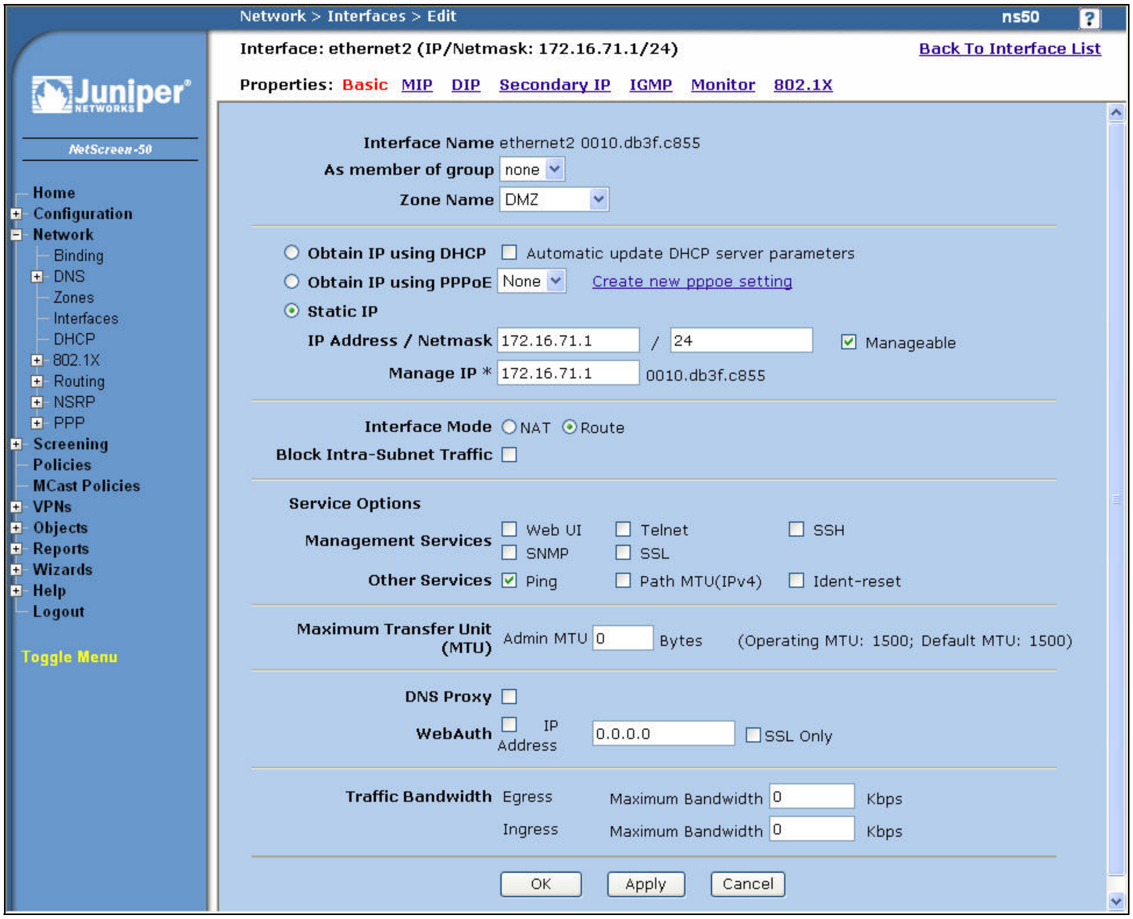
| Step | Description |
|---|---|
| 1. | The Netscreen 50 is configured via a web browser. To access the web interface, enter http://<*ip-addr*> in the address field of the web browser, where <*ip-addr*> is the IP address of the Netscreen 50.<br>Log in with the appropriate credentials. Click **Login**.<br><br> Admin Name:<br>Password:<br>□ Remember my name and password<br>Login |

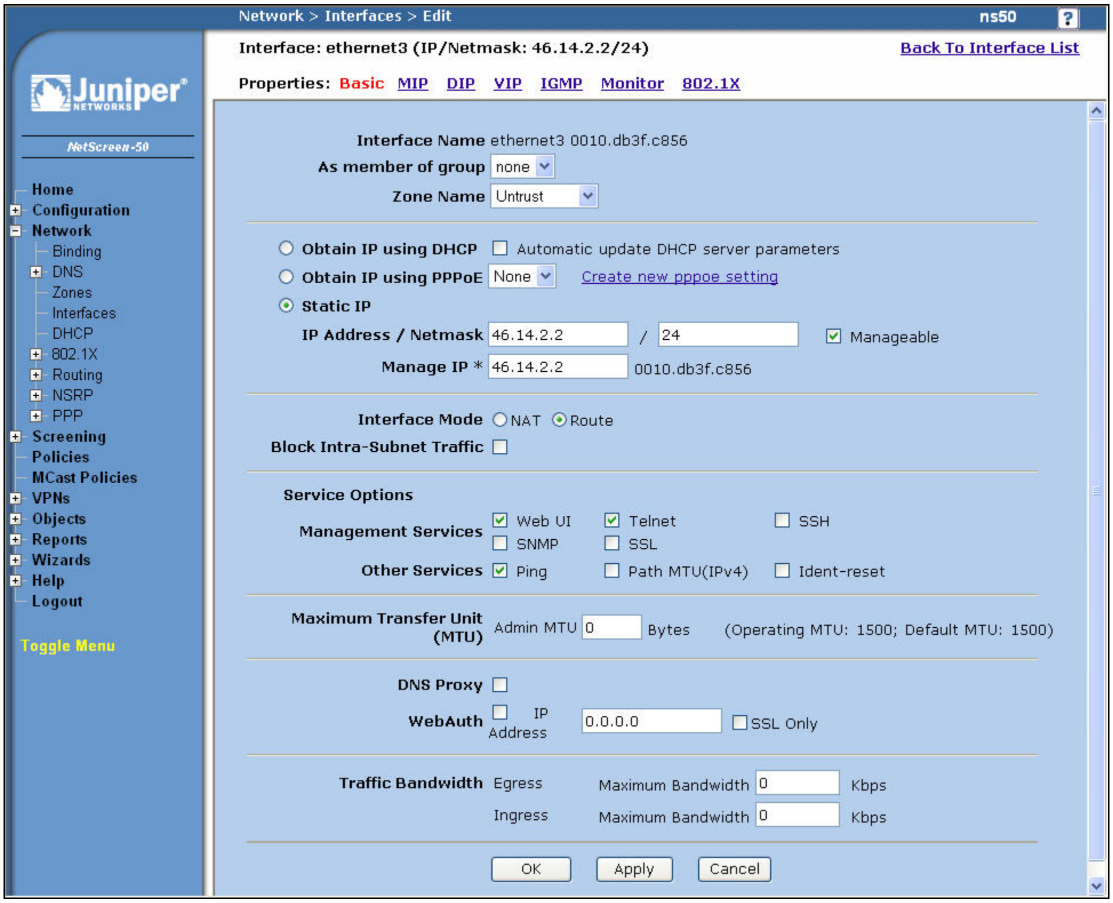
| Step | Description |
|---|---|
| 2. | The main page appears as shown below.<br><br>Home ns50<br>Up time: 1 day 19:09:17, System time: 2007-03-28 09:45:16 GMT Time Zone 00:00<br>manually Refresh<br>**Device Information**<br>Hardware Version: 4010(0)<br>Firmware Version: 5.4.0r1.0 (Firewall+VPN)<br>Serial Number: 0019032003000254<br>Host Name: ns50<br>**System Status (Root)**<br>Administrator: netscreen<br>Current Logins: 1 Details<br>**Resources Status**<br>CPU:<br>Memory:<br>Sessions:<br>Policies:<br>Start from here...<br>Interface link status: More...<br>Name / Zone / Link<br>ethernet1 / Trust / Up<br>ethernet2 / DMZ / Up<br>ethernet3 / Untrust / Up<br>The most recent alarms: More...<br>Date/Time / Level / Description<br>No entry available.<br>The most recent events: More...<br>Date/Time / Level / Description<br>2007-03-28 09:45:14 / warn / Admin user "netscreen" logged in for Web...<br>2007-03-26 18:10:25 / notif / The physical state of interface ethernet...<br>2007-03-26 18:10:16 / notif / The physical state of interface ethernet...<br>2007-03-26 18:07:25 / notif / The physical state of interface ethernet...<br>2007-03-26 18:05:55 / notif / The physical state of interface ethernet...<br> Juniper NETWORKS<br>NetScreen-50<br>Home<br>Configuration<br>Network<br>Screening<br>Policies<br>MCast Policies<br>VPNs<br>Objects<br>Reports<br>Wizards<br>Help<br>Logout<br>Toggle Menu |
| 3. | **Application Layer Gateway (ALG)**<br>The SIP ALG function must be disabled. From the left pane, navigate to **Configuration→Advanced→ALG→Configure**. Uncheck the box next to **SIP**. The other settings can remain unchanged. Click **Apply**.<br><br>Configuration > Advanced > ALG >Basic ns50<br>Basic MGCP H323 SIP SCCP<br>**Application Layer Gateway**<br>□ SIP<br>□ SCCP<br>□ H323<br>□ Microsoft RPC<br>□ Sun RPC<br>□ RTSP<br>□ SQL<br>□ MGCP<br> Apply<br>Cancel<br>Juniper NETWORKS<br>NetScreen-50<br>Home<br>Configuration<br>Date/Time<br>Update<br>Admin<br>Auth<br>Infranet Auth<br>Report Settings<br>Advanced<br>Traffic Shaping<br>ALG<br>Configure<br>Flow<br>Network<br>Screening |

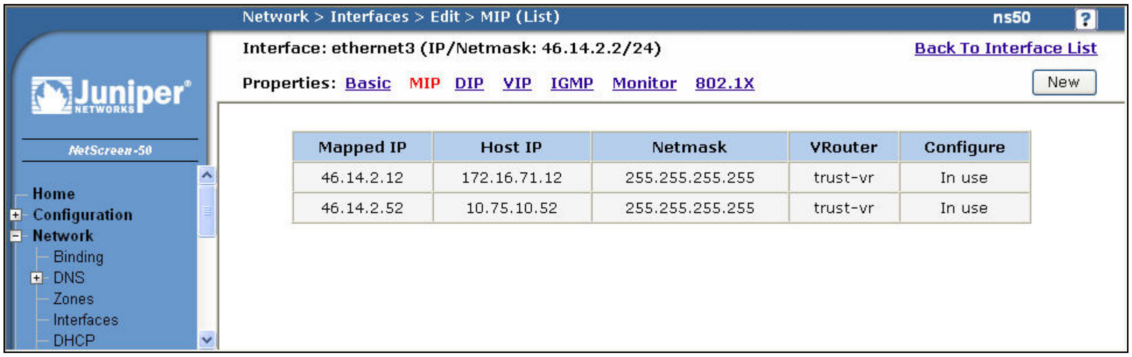
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>
<b>Interfaces</b><br>
To configure the interfaces of the firewall, navigate to <b>Network→Interfaces</b> in the left pane of the window. As a result of the factory defaults, four interfaces named ethernet1 – ethernet4, that correspond to the four physical ports on the device, will appear in the table in the right pane. Other logical interfaces may also be present.<br><br>
For the compliance test, interfaces ethernet1 – ethernet3 were used. The example below shows the interface list after these interfaces were configured for testing. To view the configuration of each interface, click <b>Edit</b> next to the interface of interest.<br><br>


Network &gt; Interfaces (List)<br>
List 20 per page<br>
List ALL(5) Interfaces<br>
<table>
<tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr>
<tr><td>ethernet1</td><td>10.75.1.254/24</td><td>Trust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet2</td><td>172.16.71.1/24</td><td>DMZ</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet3</td><td>46.14.2.2/24</td><td>Untrust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet4</td><td>0.0.0.0/0</td><td>Null</td><td>Unused</td><td>Down</td><td>-</td><td>Edit</td></tr>
<tr><td>vlan1</td><td>192.168.1.250/24</td><td>VLAN</td><td>Layer3</td><td>Down</td><td>-</td><td>Edit</td></tr>
</table>
</td></tr>
</table>

| Step | Description |
|---|---|
| 5. | **Interface – ethernet1 (Private)**<br>The interface, ethernet1, was configured as follows:<br>• **Zone Name**: ***Trust*** This is the private side of the firewall.<br>• **Static IP**: Select this radio button.<br>• **IP Address / Netmask**: Enter the IP address and netmask for the private side of the firewall.<br>• **Manageable**: Check this box to allow the firewall to be managed from this interface. The compliance test used this interface to manage the device.<br>• **Manage IP**: If the **Manageable** box is checked, enter the same address as used in the **IP Address** field.<br>• **Interface Mode**: Select the **Route** button.<br>• **Service Options**: Check the box next to any service that will be available on this interface.<br><br>Click **OK**.<br><br>Network > Interfaces > Edit ns50<br>Interface: ethernet1 (IP/Netmask: 10.75.1.254/24) Back To Interface List<br>Properties: Basic MIP DIP Secondary IP IGMP Monitor 802.1X<br>Interface Name ethernet1 0010.db3f.c850<br>As member of group none<br>Zone Name Trust<br>○ Obtain IP using DHCP □ Automatic update DHCP server parameters<br>○ Obtain IP using PPPoE None Create new pppoe setting<br>● Static IP<br>IP Address / Netmask 10.75.1.254 / 24 ☑ Manageable<br>Manage IP * 10.75.1.254 0010.db3f.c850<br>Interface Mode ○ NAT ● Route<br>Block Intra-Subnet Traffic □<br>Service Options<br>Management Services ☑ Web UI ☑ Telnet ☑ SSH ☑ SNMP ☑ SSL<br>Other Services ☑ Ping □ Path MTU(IPv4) □ Ident-reset<br>Maximum Transfer Unit (MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)<br>DNS Proxy □<br>WebAuth □ IP Address 0.0.0.0 □ SSL Only<br>Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps<br>Ingress Maximum Bandwidth 0 Kbps<br> Juniper NETWORKS<br>NetScreen-50<br>Home<br>Configuration<br>Network<br>Binding<br>DNS<br>Zones<br>Interfaces<br>DHCP<br>802.1X<br>Routing<br>NSRP<br>PPP<br>Screening<br>Policies<br>MCast Policies<br>VPNs<br>Objects<br>Reports<br>Wizards<br>Help<br>Logout<br>Toggle Menu<br>OK<br>Apply<br>Cancel |

| Step | Description |
|---|---|
| 6. | **Interface – ethernet2 (DMZ)**<br>The interface, ethernet2, was configured as follows:<br>- **Zone Name**: ***DMZ*** This is the zone which will contain IPCS.<br>- **Static IP**: Select this radio button.<br>- **IP Address / Netmask**: Enter the IP address and netmask for the DMZ of the firewall.<br>- **Manageable**: Check this box to allow the firewall to be managed from this interface. This was not required for the compliance test but was enabled.<br>- **Manage IP**: If the **Manageable** box is checked, enter the same address as used in the **IP Address** field.<br>- **Interface Mode**: Select the **Route** button.<br>- **Service Options**: Check the box next to any service that will be available on this interface.<br><br>Click **OK**.<br><br> Juniper NETWORKS<br>NetScreen-50<br>Home<br>Configuration<br>Network<br>Binding<br>DNS<br>Zones<br>Interfaces<br>DHCP<br>802.1X<br>Routing<br>NSRP<br>PPP<br>Screening<br>Policies<br>MCast Policies<br>VPNs<br>Objects<br>Reports<br>Wizards<br>Help<br>Logout<br>Toggle Menu<br>Network > Interfaces > Edit ns50<br>Interface: ethernet2 (IP/Netmask: 172.16.71.1/24) Back To Interface List<br>Properties: Basic MIP DIP Secondary IP IGMP Monitor 802.1X<br>Interface Name ethernet2 0010.db3f.c855<br>As member of group none<br>Zone Name DMZ<br>○ Obtain IP using DHCP □ Automatic update DHCP server parameters<br>○ Obtain IP using PPPoE None Create new pppoe setting<br>● Static IP<br>IP Address / Netmask 172.16.71.1 / 24 ☑ Manageable<br>Manage IP * 172.16.71.1 0010.db3f.c855<br>Interface Mode ○ NAT ● Route<br>Block Intra-Subnet Traffic □<br>Service Options<br>Management Services □ Web UI □ Telnet □ SSH<br>□ SNMP □ SSL<br>Other Services ☑ Ping □ Path MTU(IPv4) □ Ident-reset<br>Maximum Transfer Unit (MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)<br>DNS Proxy □<br>WebAuth □ IP Address 0.0.0.0 □ SSL Only<br>Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps<br>Ingress Maximum Bandwidth 0 Kbps<br>OK Apply Cancel |

| Step | Description |
|---|---|
| 7. | **Interface – ethernet3 (Public)**<br>The interface, ethernet3, was configured as follows:<br>• **Zone Name**: ***Untrust*** This is the public side of the firewall.<br>• **Static IP**: Select this radio button.<br>• **IP Address / Netmask**: Enter the IP address and netmask for the DMZ of the firewall.<br>• **Manageable**: Check this box to allow the firewall to be managed from this interface. This was not required for the compliance test but was enabled.<br>• **Manage IP**: If the **Manageable** box is checked, enter the same address as used in the **IP Address** field.<br>• **Interface Mode**: Select the **Route** button.<br>• **Service Options**: Check the box next to any service that will be available on this interface.<br>Network address translation is performed on this interface. However, instead of setting the **Interface Mode** above to NAT, a static translation is defined using mapped IP (MIP) addresses. Select the **MIP** link at the top of the page to define these mappings.<br><br>Network > Interfaces > Edit ns50<br>Interface: ethernet3 (IP/Netmask: 46.14.2.2/24) Back To Interface List<br>Properties: Basic MIP DIP VIP IGMP Monitor 802.1X<br>Interface Name ethernet3 0010.db3f.c856<br>As member of group none<br>Zone Name Untrust<br>○ Obtain IP using DHCP □ Automatic update DHCP server parameters<br>○ Obtain IP using PPPoE None Create new pppoe setting<br>● Static IP<br>IP Address / Netmask 46.14.2.2 / 24 ☑ Manageable<br>Manage IP * 46.14.2.2 0010.db3f.c856<br>Interface Mode ○ NAT ● Route<br>Block Intra-Subnet Traffic □<br>Service Options<br>Management Services ☑ Web UI ☑ Telnet □ SSH □ SNMP □ SSL<br>Other Services ☑ Ping □ Path MTU(IPv4) □ Ident-reset<br>Maximum Transfer Unit (MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)<br>DNS Proxy □<br>WebAuth □ IP Address 0.0.0.0 □ SSL Only<br>Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps<br>Ingress Maximum Bandwidth 0 Kbps<br> NetScreen-50<br>Home<br>Configuration<br>Network<br>Binding<br>DNS<br>Zones<br>Interfaces<br>DHCP<br>802.1X<br>Routing<br>NSRP<br>PPP<br>Screening<br>Policies<br>MCast Policies<br>VPNs<br>Objects<br>Reports<br>Wizards<br>Help<br>Logout<br>Toggle Menu<br>OK<br>Apply<br>Cancel |

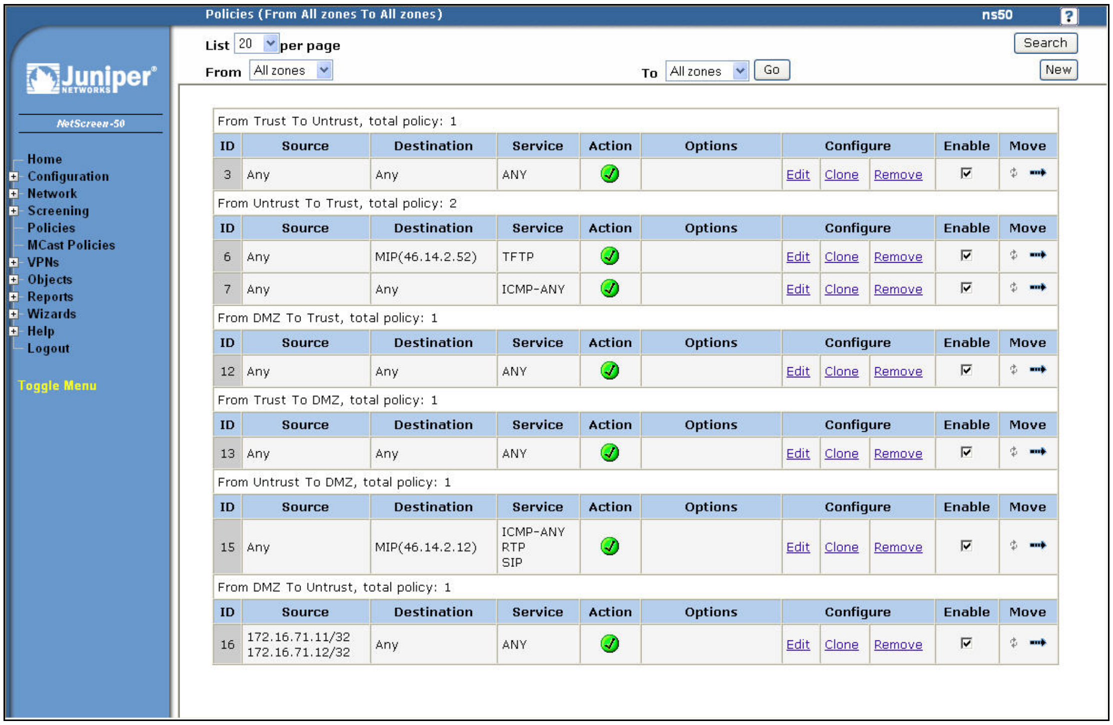
| Step | Description |
|---|---|
| 8. | **Mapped IP addresses (MIP)**<br>Mapped IP addresses were used to map a public accessible IP address to a host IP address on the private or DMZ side of the firewall. Each mapping was created by selecting the **New** button. A new page is opened (not shown) where the address mapping information can be entered and submitted.<br>The MIP list below shows the mapped IP addresses used for the compliance test. The first entry maps a public IP address to the public side of IPCS which resides in the DMZ. The second entry maps a public IP to the internal IP address of the TFTP server. The **Netmask** value of ***255.255.255.255*** used in each entry indicates that a single IP address, not a range of addresses, is being mapped with that particular entry. The **VRouter** field refers to the virtual router used. Only one virtual router, ***trust-vr***, was used in the compliance test, so both entries were set to this value. More information on the topic of virtual routers can be obtained from [7].<br>After creating the MIPs, click on the **Basic** link to return to the previous page. On the **Basic** page, click **OK**.<br> |

Network > Interfaces > Edit > MIP (List)

Interface: ethernet3 (IP/Netmask: 46.14.2.2/24)

Properties: Basic MIP DIP VIP IGMP Monitor 802.1X

| Mapped IP | Host IP | Netmask | VRouter | Configure |
|---|---|---|---|---|
| 46.14.2.12 | 172.16.71.12 | 255.255.255.255 | trust-vr | In use |
| 46.14.2.52 | 10.75.10.52 | 255.255.255.255 | trust-vr | In use |

| Step | Description |
|---|---|
| 9. | **Policies**<br>Policies define the traffic that is allowed to flow through the firewall. To configure a policy, navigate to **Policies** in the left pane. Each policy is created by selecting a **From** zone and a **To** zone from the pull-downs at the top of the **Policies** page and clicking the **New** button. A new page is opened (not shown) where the policy information can be entered and submitted.<br><br>The list below shows the policies used for the compliance test. **Steps 4 – 7** have previously defined the following:<br>• Trust zone: Connects to the private enterprise LAN.<br>• DMZ zone: Connects to IPCS.<br>• Untrust zone: Connects to the public untrusted IP network.<br><br>The policies used in the compliance test are summarized as follows:<br>• Policy 3, 12, and 13: Traffic is unrestricted in the direction of Trust to Untrust, DMZ to Trust and Trust to DMZ.<br>• Policy 6: TFTP traffic to the public MIP of the TFTP server is allowed from the Untrust to Trust zone.<br>• Policy 7: ICMP traffic (for pings) is allowed from the Untrust to Trust zone. This is not required for the compliance test but used for troubleshooting of the configuration.<br>• Policy 15: SIP, RTP and ICMP traffic (for pings) to the public mapped IP address of IPCS is allowed from the Untrust to DMZ zones. The ICMP traffic is not required for the compliance test.<br>• Policy 16: Any traffic from either IP address of IPCS is allowed from the DMZ to Untrust zone.<br> |

Policies (From All zones To All zones)

List 20 per page

From All zones To All zones

From Trust To Untrust, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | Any | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

From Untrust To Trust, total policy: 2

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | Any | MIP(46.14.2.52) | TFTP | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |
| 7 | Any | Any | ICMP-ANY | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

From DMZ To Trust, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 12 | Any | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

From Trust To DMZ, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 13 | Any | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

From Untrust To DMZ, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 15 | Any | MIP(46.14.2.12) | ICMP-ANY<br>RTP<br>SIP | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

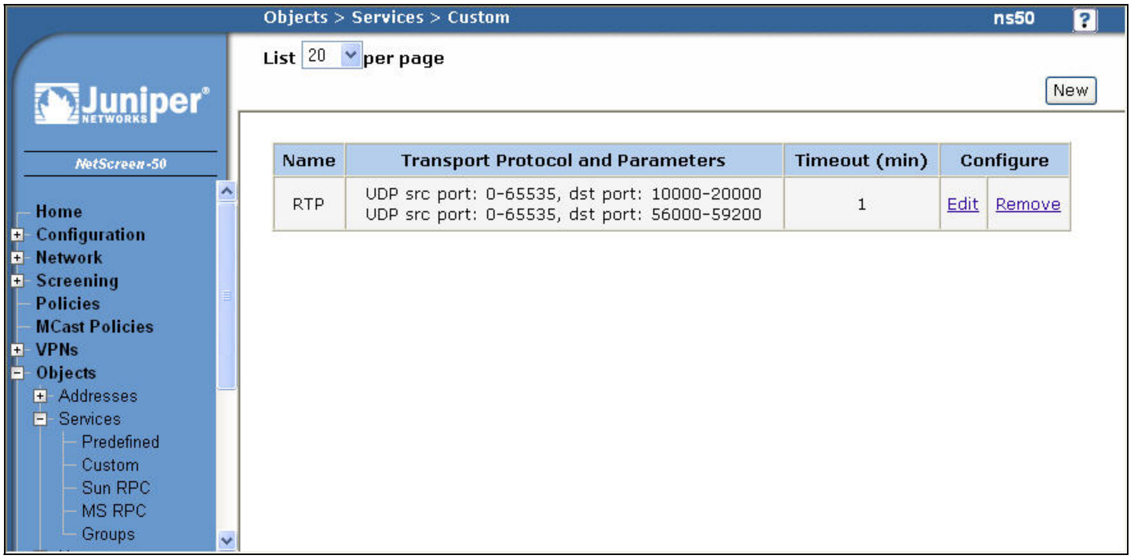
From DMZ To Untrust, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 172.16.71.11/32<br>172.16.71.12/32 | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ | ⇕ ➡ |

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>10.</td><td>

**Services**
The services used in the policies in **Step 9** were standard services defined by the firewall with the exception of the service called RTP. RTP does not use a set of well known ports, so a custom service must be created by the user to define the ports and transport protocol that define the service RTP. To create a custom service, navigate to **Objects→Services→Custom** from the left pane. Click on the **New** button. A new page is opened (not shown) where the policy information can be entered and submitted.

The table below shows the custom service named RTP used for the compliance test. It shows the source port as any valid UDP port and the destination port as any UDP port between 10000 – 20000 or 56000 - 59200. These ports were chosen based on default values used by IPCS for RTP traffic. The range of ports used can be further restricted as long as the range of ports are compatible to the ports used by IPCS and the remote endpoints. Even though the range of ports used by the compliance test was large, the firewall policy only allows this traffic to a single host (IPCS).



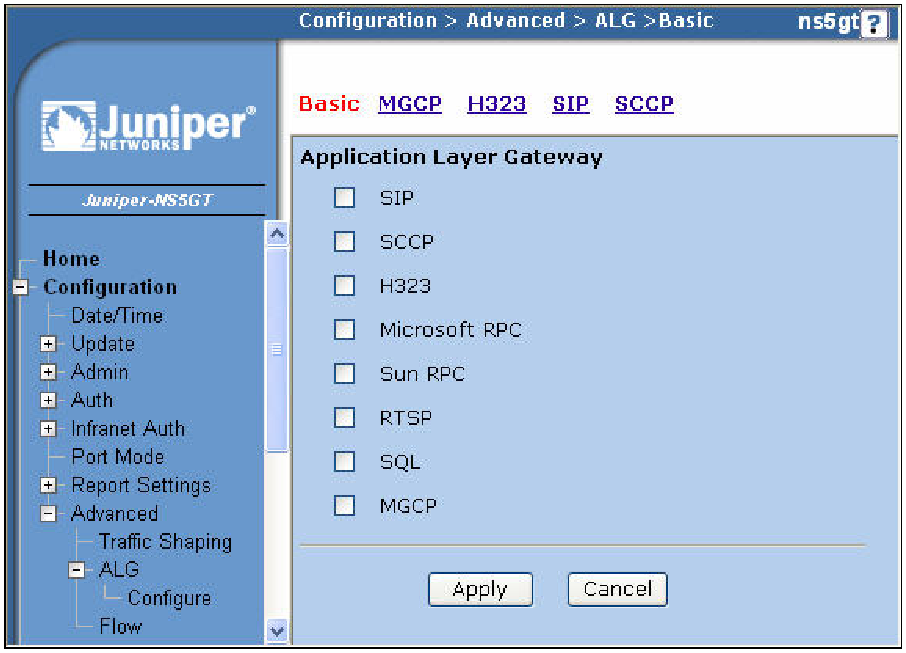
List 20 per page

<table>
<tr><th>Name</th><th>Transport Protocol and Parameters</th><th>Timeout (min)</th><th colspan="2">Configure</th></tr>
<tr><td>RTP</td><td>UDP src port: 0-65535, dst port: 10000-20000<br>UDP src port: 0-65535, dst port: 56000-59200</td><td>1</td><td>Edit</td><td>Remove</td></tr>
</table>

</td></tr>
</table>

## 7. Configure Juniper Networks Netscreen 5GT

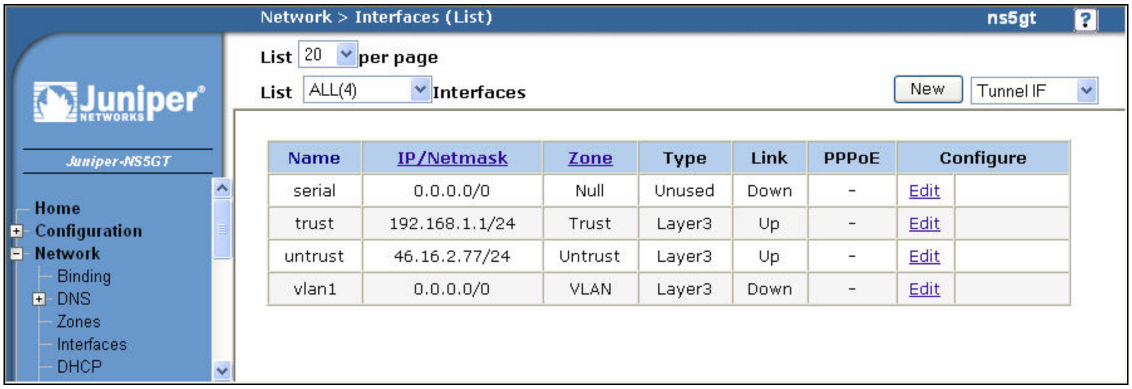
This section covers the configuration of the Netscreen 5GT firewall. The configuration was the same for both Netscreen 5GT firewalls shown in **Figure 1** with the exception of the IP addresses used.

| Step | Description |
|---|---|
| 1. | The Netscreen 5GT is configured via a web browser. It is accessed in the same manner as the Netscreen 50. |
| 2. | **Application Layer Gateway (ALG)**<br>The SIP ALG function must be disabled. From the left pane, navigate to **Configuration→Advanced→ALG→Configure**. Uncheck the box next to **SIP**. The other settings can remain unchanged. Click **Apply**.<br><br> Configuration > Advanced > ALG >Basic<br>ns5gt<br>Juniper NETWORKS<br>Juniper-NS5GT<br>Home<br>Configuration<br>Date/Time<br>Update<br>Admin<br>Auth<br>Infranet Auth<br>Port Mode<br>Report Settings<br>Advanced<br>Traffic Shaping<br>ALG<br>Configure<br>Flow<br>Basic<br>MGCP<br>H323<br>SIP<br>SCCP<br>Apply<br>Cancel<br>Application Layer Gateway<br>□ SIP<br>□ SCCP<br>□ H323<br>□ Microsoft RPC<br>□ Sun RPC<br>□ RTSP<br>□ SQL<br>□ MGCP |

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

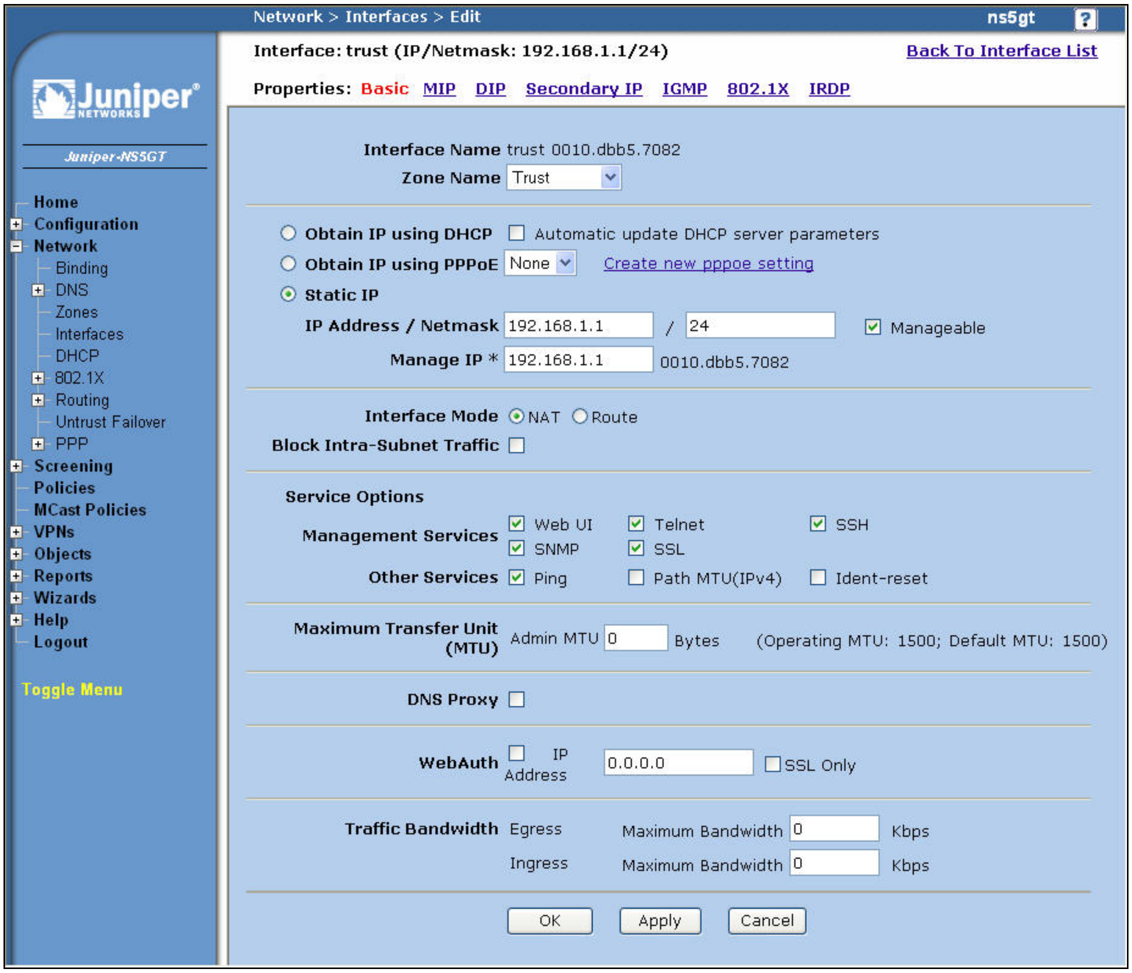
**Interfaces**<br>
To configure the interfaces of the firewall, navigate to **Network→Interfaces** in the left pane of the window.  As a result of the factory defaults, several interfaces will automatically appear in the table.

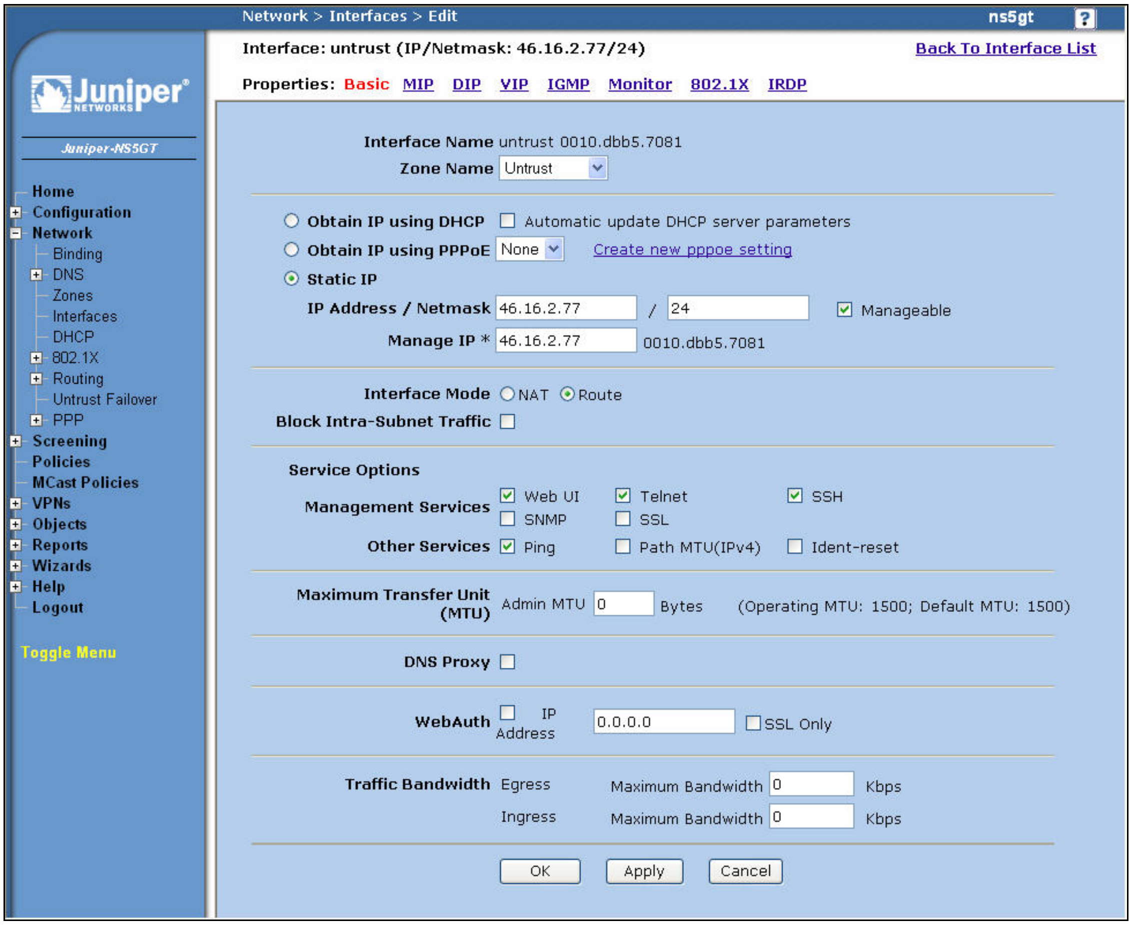
For the compliance test, interfaces trust and untrust were used.  The **trust** interface corresponds to the four Ethernet switch ports labeled 1 – 4 on the device.  The **untrust** interface corresponds to the physical port labeled untrusted on the device. The example below shows the interface list after these interfaces were configured for testing.  To view the configuration of each interface, click **Edit** next to the interface of interest.



<table>
<tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr>
<tr><td>serial</td><td>0.0.0.0/0</td><td>Null</td><td>Unused</td><td>Down</td><td>-</td><td>Edit</td></tr>
<tr><td>trust</td><td>192.168.1.1/24</td><td>Trust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>untrust</td><td>46.16.2.77/24</td><td>Untrust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>vlan1</td><td>0.0.0.0/0</td><td>VLAN</td><td>Layer3</td><td>Down</td><td>-</td><td>Edit</td></tr>
</table>

</td></tr>
</table>

| Step | Description |
|---|---|
| 4. | **Interface – trust (Private)**<br>The interface, trust, was configured as follows:<br>• **Zone Name**: ***Trust*** This is the private side of the firewall.<br>• **Static IP**: Select this radio button.<br>• **IP Address / Netmask**: Enter the IP address and netmask for the private side of the firewall.<br>• **Manageable**: Check this box to allow the firewall to be managed from this interface. The compliance test used this interface to manage the device.<br>• **Manage IP**: If the **Manageable** box is checked, enter the same address as used in the **IP Address** field.<br>• **Interface Mode**: Select the **NAT** button.<br>• **Service Options**: Check the box next to any service that will be available on this interface.<br>Click **OK**.<br><br>Network > Interfaces > Edit ns5gt<br>Interface: trust (IP/Netmask: 192.168.1.1/24) Back To Interface List<br>Properties: Basic MIP DIP Secondary IP IGMP 802.1X IRDP<br>Interface Name trust 0010.dbb5.7082<br>Zone Name Trust<br>○ Obtain IP using DHCP □ Automatic update DHCP server parameters<br>○ Obtain IP using PPPoE None Create new pppoe setting<br>● Static IP<br>IP Address / Netmask 192.168.1.1 / 24 ☑ Manageable<br>Manage IP * 192.168.1.1 0010.dbb5.7082<br>Interface Mode ● NAT ○ Route<br>Block Intra-Subnet Traffic □<br>Service Options<br>Management Services ☑ Web UI ☑ Telnet ☑ SSH ☑ SNMP ☑ SSL<br>Other Services ☑ Ping □ Path MTU(IPv4) □ Ident-reset<br>Maximum Transfer Unit (MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)<br>DNS Proxy □<br>WebAuth □ IP Address 0.0.0.0 □ SSL Only<br>Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps<br>Ingress Maximum Bandwidth 0 Kbps<br> Juniper NETWORKS<br>Juniper-NS5GT<br>Home<br>Configuration<br>Network<br>Binding<br>DNS<br>Zones<br>Interfaces<br>DHCP<br>802.1X<br>Routing<br>Untrust Failover<br>PPP<br>Screening<br>Policies<br>MCast Policies<br>VPNs<br>Objects<br>Reports<br>Wizards<br>Help<br>Logout<br>Toggle Menu<br>OK<br>Apply<br>Cancel |

| Step | Description |
|---|---|
| 5. | **Interface – untrust (Public)**<br>The interface, untrust, was configured as follows:<br>• **Zone Name**: ***Untrust*** This is the public side of the firewall.<br>• **Static IP**: Select this radio button.<br>• **IP Address / Netmask**: Enter the IP address and netmask for the DMZ of the firewall.<br>• **Manageable**: Check this box to allow the firewall to be managed from this interface. This was not required for the compliance test but was enabled.<br>• **Manage IP**: If the **Manageable** box is checked, enter the same address as used in the **IP Address** field.<br>• **Interface Mode**: Select the **Route** button.<br>• **Service Options**: Check the box next to any service that will be available on this interface.<br><br>Click **OK**.<br> |

Network > Interfaces > Edit — ns5gt

Interface: untrust (IP/Netmask: 46.16.2.77/24) — Back To Interface List

Properties: Basic MIP DIP VIP IGMP Monitor 802.1X IRDP

Interface Name untrust 0010.dbb5.7081
Zone Name Untrust

○ Obtain IP using DHCP □ Automatic update DHCP server parameters
○ Obtain IP using PPPoE None Create new pppoe setting
● Static IP
IP Address / Netmask 46.16.2.77 / 24 ☑ Manageable
Manage IP * 46.16.2.77 0010.dbb5.7081

Interface Mode ○ NAT ● Route
Block Intra-Subnet Traffic □

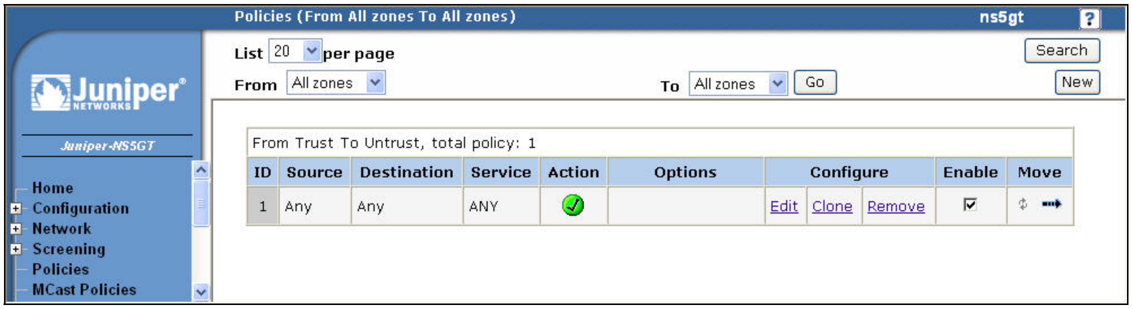
Service Options
Management Services ☑ Web UI ☑ Telnet ☑ SSH □ SNMP □ SSL
Other Services ☑ Ping □ Path MTU(IPv4) □ Ident-reset

Maximum Transfer Unit (MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy □

WebAuth □ IP Address 0.0.0.0 □ SSL Only

Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps
Ingress Maximum Bandwidth 0 Kbps

| Step | Description |
|---|---|
| 6. | **Policies**<br>Policies define the traffic that is allowed to flow through the firewall. To configure a policy, navigate to **Policies** in the left pane. Each policy is created by selecting a **From** zone and a **To** zone from the pull-downs at the top of the **Policies** page and clicking the **New** button. A new page is opened (not shown) where the policy information can be entered and submitted.<br>The list below shows the policies used for the compliance test. **Steps 3 – 5** have previously defined the following:<br>• Trust zone: Connects to the private enterprise LAN.<br>• Untrust zone: Connects to the public untrusted IP network.<br>The policies used in the compliance test are summarized as follows:<br>• Policy 1: Traffic is unrestricted in the direction of Trust to Untrust.<br> |

Policies (From All zones To All zones)

List 20 per page

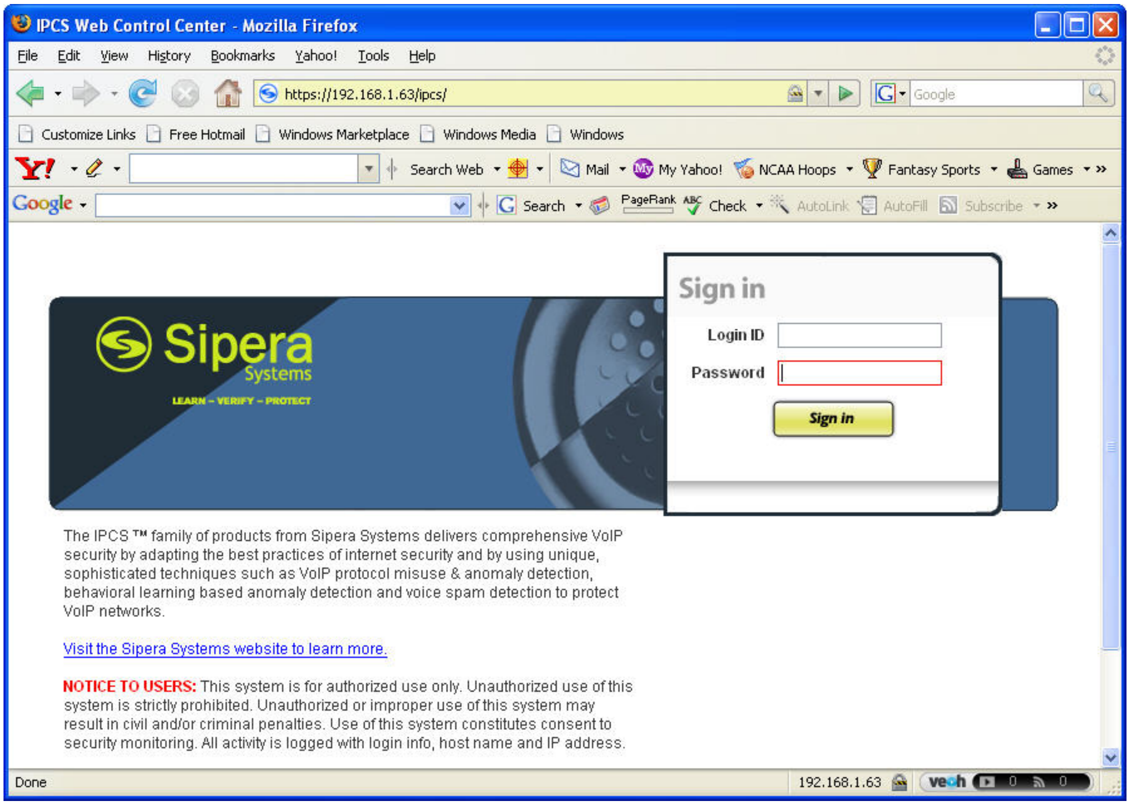
From All zones To All zones

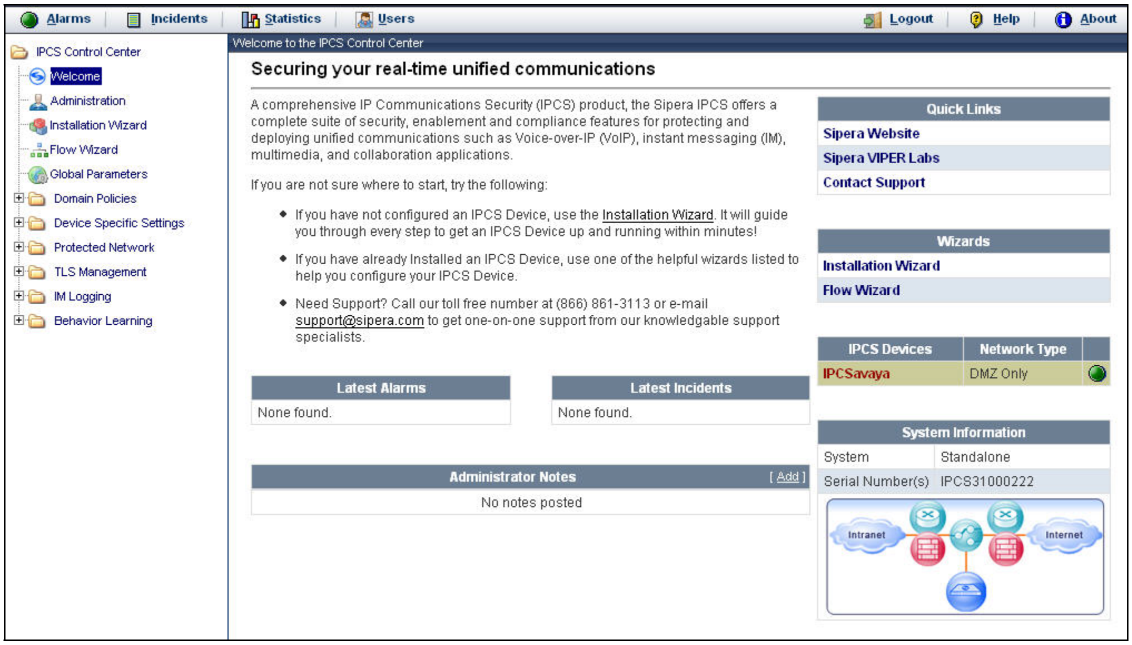
From Trust To Untrust, total policy: 1

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable | Move |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Any | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ | |

## 8. Configure Sipera IPCS

This section covers the configuration of IPCS. It is assumed that the IPCS software has already been installed. For additional information on these installation tasks, refer to [8].

| Step | Description |
|---|---|
| 1. | IPCS is configured via the Mozilla Firefox web browser. IPCS does not support Internet Explorer. To access the web interface, enter https://*<ip-addr>*/ipcs in the address field of the web browser, where *<ip-addr>* is the IP address of IPCS.<br>Log in with the appropriate credentials. Click **Sign In**.<br><br>IPCS Web Control Center - Mozilla Firefox<br>https://192.168.1.63/ipcs/<br>The IPCS ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.<br>Visit the Sipera Systems website to learn more.<br>NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.<br> File Edit View History Bookmarks Yahoo! Tools Help<br>Sipera Systems<br>LEARN – VERIFY – PROTECT<br>Sign in<br>Login ID<br>Password<br>Sign in<br>Done<br>192.168.1.63 |

| Step | Description |
|---|---|
| 2. | The main page of the IPCS Control Center will appear.<br> |

Welcome to the IPCS Control Center

Securing your real-time unified communications

A comprehensive IP Communications Security (IPCS) product, the Sipera IPCS offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you are not sure where to start, try the following:

- If you have not configured an IPCS Device, use the Installation Wizard. It will guide you through every step to get an IPCS Device up and running within minutes!
- If you have already Installed an IPCS Device, use one of the helpful wizards listed to help you configure your IPCS Device.
- Need Support? Call our toll free number at (866) 861-3113 or e-mail support@sipera.com to get one-on-one support from our knowledgable support specialists.

| Quick Links |
|---|
| Sipera Website |
| Sipera VIPER Labs |
| Contact Support |

| Wizards |
|---|
| Installation Wizard |
| Flow Wizard |

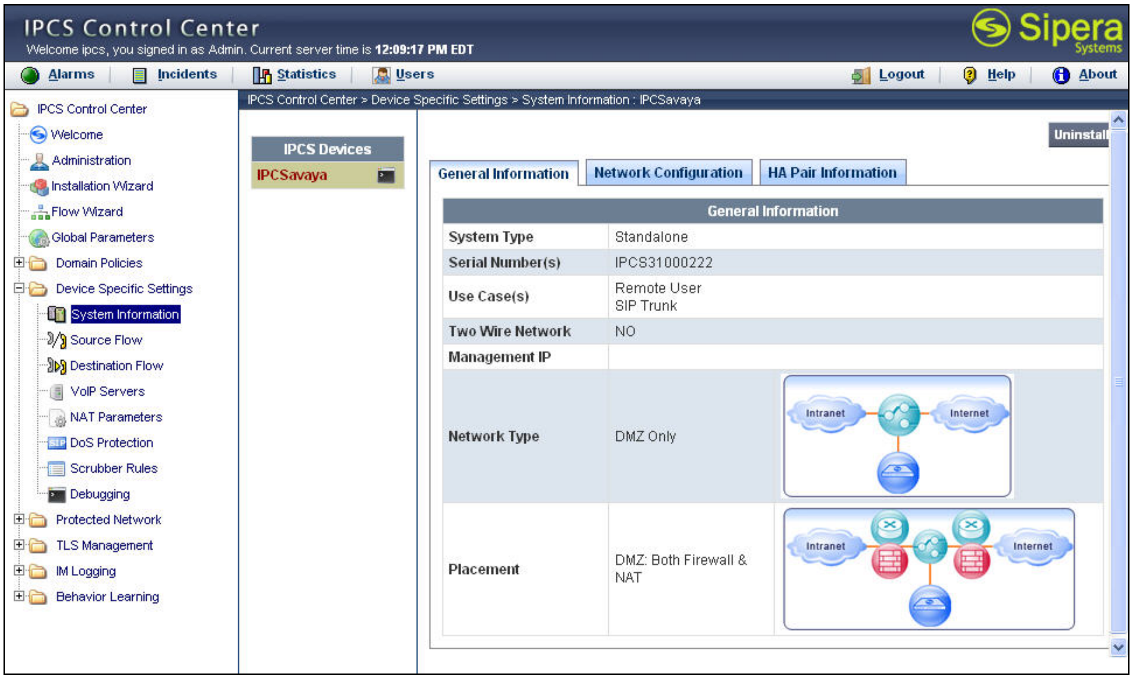
| IPCS Devices | Network Type | |
|---|---|---|
| IPCSavaya | DMZ Only | ● |

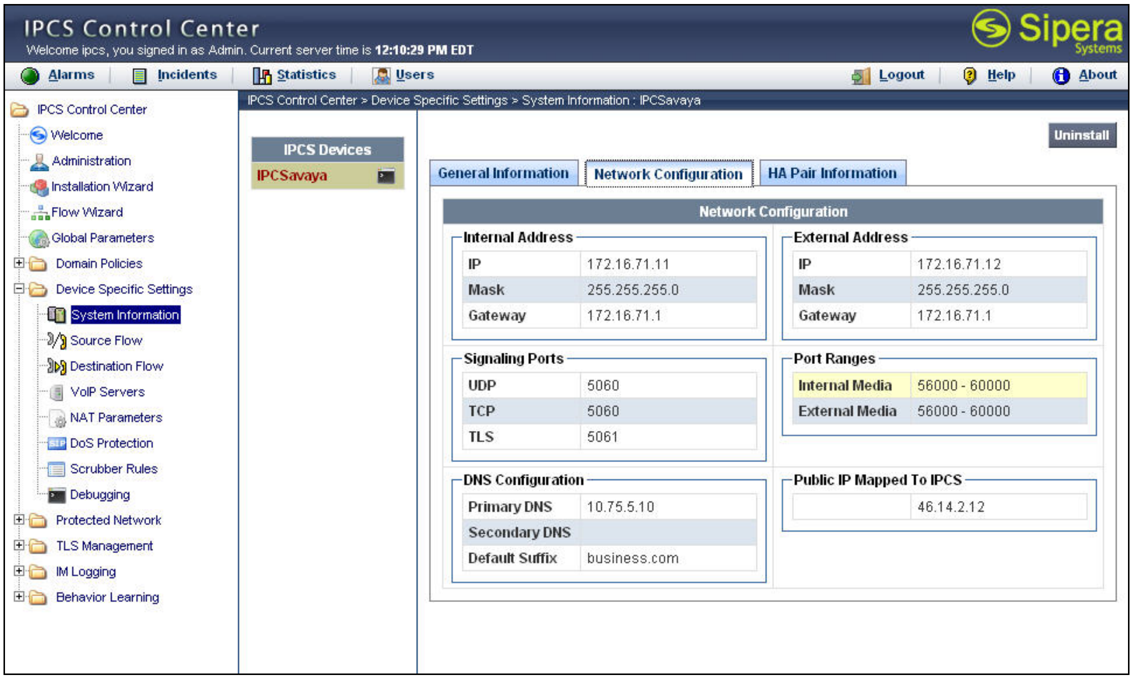
| Latest Alarms |
|---|
| None found. |

| Latest Incidents |
|---|
| None found. |

| Administrator Notes [ Add ] |
|---|
| No notes posted |

| System Information | |
|---|---|
| System | Standalone |
| Serial Number(s) | IPCS31000222 |

| Step | Description |
|---|---|
| 3. | To view system information that was configured during installation, navigate to **IPCS Control Center→Device Specific Settings→System Information**. From the list of **IPCS Devices** in the middle pane, select the only IPCS used in this configuration named ***IPCSavaya***. The system information is shown in the right pane. The **General Information** tab shows the values of the following key parameters.<br>• **System Type**: ***Standalone***<br>• **Network Type**: ***DMZ Only***<br>• **Placement**: ***DMZ: Both Firewall & NAT***<br><br>Click the **Network Configuration** tab to view the network settings.<br><br>IPCS Control Center<br>Welcome ipcs, you signed in as Admin. Current server time is **12:09:17 PM EDT**<br>Alarms \| Incidents \| Statistics \| Users \| Logout \| Help \| About<br>IPCS Control Center > Device Specific Settings > System Information : IPCSavaya<br>IPCS Control Center: Welcome, Administration, Installation Wizard, Flow Wizard, Global Parameters, Domain Policies, Device Specific Settings (System Information, Source Flow, Destination Flow, VoIP Servers, NAT Parameters, DoS Protection, Scrubber Rules, Debugging), Protected Network, TLS Management, IM Logging, Behavior Learning<br>IPCS Devices: IPCSavaya<br>Uninstall<br>General Information \| Network Configuration \| HA Pair Information<br>**General Information**<br>System Type: Standalone<br>Serial Number(s): IPCS31000222<br>Use Case(s): Remote User, SIP Trunk<br>Two Wire Network: NO<br>Management IP:<br>Network Type: DMZ Only<br>Placement: DMZ: Both Firewall & NAT<br>Intranet<br>Internet<br>Intranet<br>Internet |

| Step | Description |
|---|---|
| 4. | The **Network Configuration** tab shows the **Internal Address**, **External Address**, and **DNS Configuration** information provided during installation and corresponds to **Figure 1**.  The compliance test did not use a DNS server, but an entry was required by IPCS.  An arbitrary IP address was used for the **Primary DNS** field, and the SIP domain was used for the **Default Suffix** field.  In addition, the **Public IP Mapped To IPCS** value was provided during installation.  Default values were used for all other fields.<br> |

Welcome ipcs, you signed in as Admin. Current server time is **12:10:29 PM EDT**

IPCS Control Center > Device Specific Settings > System Information : IPCSavaya

Network Configuration

Internal Address

| | |
|---|---|
| IP | 172.16.71.11 |
| Mask | 255.255.255.0 |
| Gateway | 172.16.71.1 |

External Address

| | |
|---|---|
| IP | 172.16.71.12 |
| Mask | 255.255.255.0 |
| Gateway | 172.16.71.1 |

Signaling Ports

| | |
|---|---|
| UDP | 5060 |
| TCP | 5060 |
| TLS | 5061 |

Port Ranges

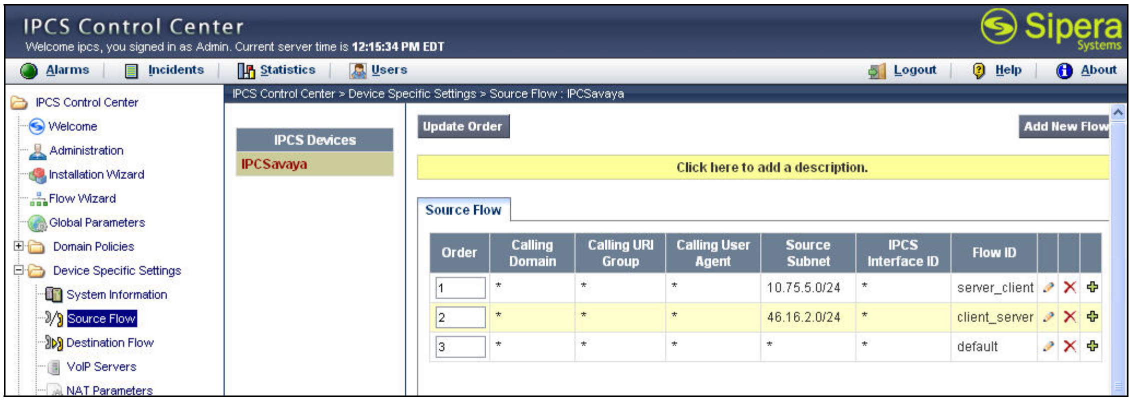
| | |
|---|---|
| Internal Media | 56000 - 60000 |
| External Media | 56000 - 60000 |

DNS Configuration

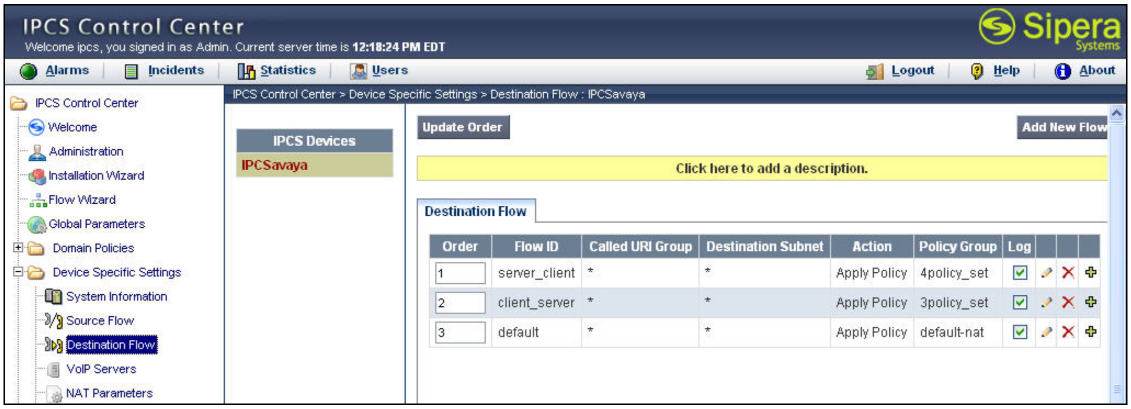
| | |
|---|---|
| Primary DNS | 10.75.5.10 |
| Secondary DNS | |
| Default Suffix | business.com |

Public IP Mapped To IPCS

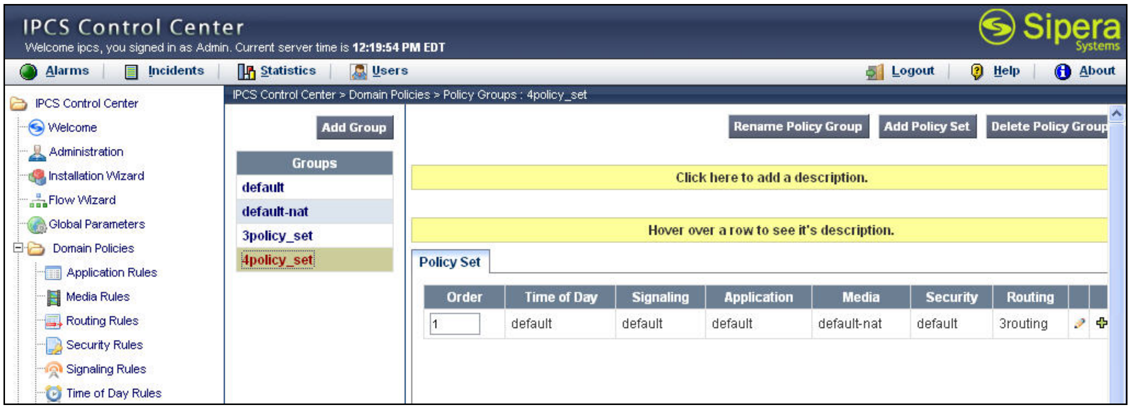
| | |
|---|---|
| | 46.14.2.12 |

| Step | Description |
|---|---|
| 5. | **Source flows**<br>A source flow defines a collection of traffic based on its source parameters and maps it to a destination flow ID. The destination flows are shown in **Step 6** and ultimately will define the policy and routing applied to the source traffic defined in the source flow.<br>To define a new source flow, navigate to **IPCS Control Center→Device Specific Settings→Source Flow**. Select the IPCS device name in the middle pane. Select the **Add New Flow** button in the right pane. A new page is opened (not shown) where the source flow information can be entered and submitted.<br>The list below shows the source flows used for the compliance test. The first entry below shows any traffic coming from **Source Subnet *10.75.5.0/24*** (private LAN side) was mapped to destination flow (**Flow ID**) ***server_client***. The second entry shows any traffic coming from **Source Subnet *46.16.2.0/24*** (public WAN side) was mapped to destination flow (**Flow ID**) ***client_server***.<br> |

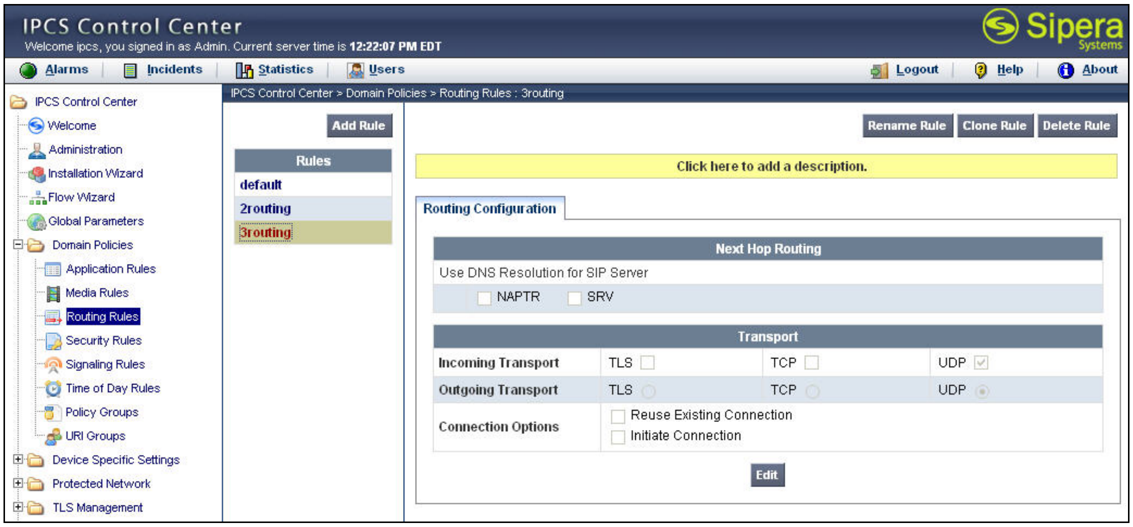
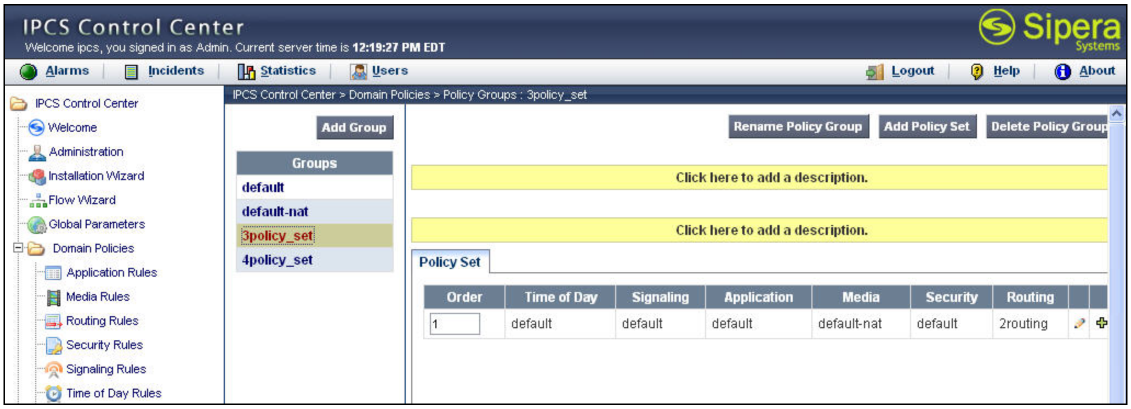
| Order | Calling Domain | Calling URI Group | Calling User Agent | Source Subnet | IPCS Interface ID | Flow ID |
|---|---|---|---|---|---|---|
| 1 | * | * | * | 10.75.5.0/24 | * | server_client |
| 2 | * | * | * | 46.16.2.0/24 | * | client_server |
| 3 | * | * | * | * | * | default |

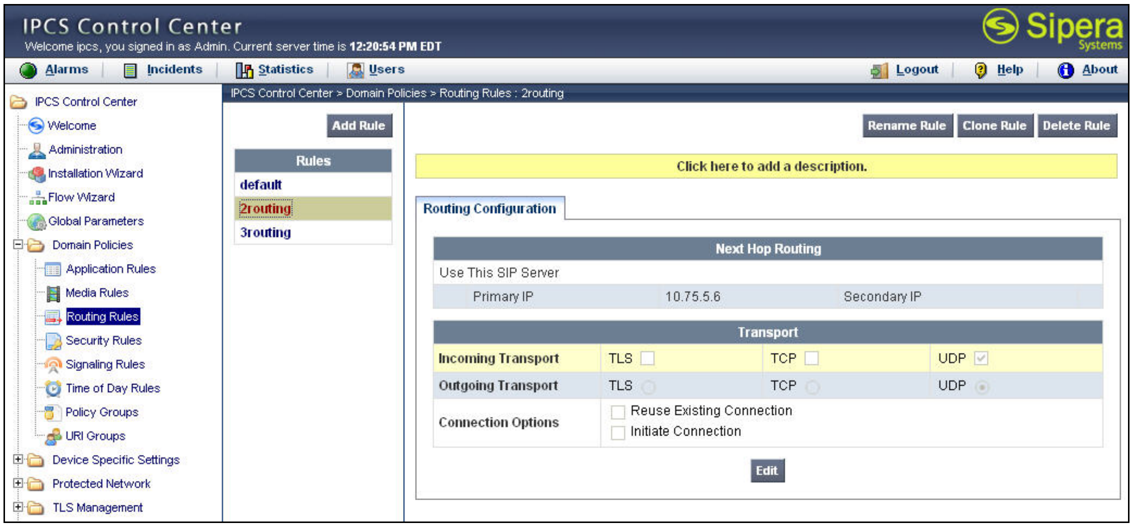
| Step | Description |
|---|---|
| 6. | **Destination Flows**<br>A destination flow defines a collection of traffic based on its destination parameters and maps a **Policy Group** and **Action** to the flow. The criteria defined in the destination flow is applied to the traffic coming from the source flow in **Step 5** which has already applied a set of criteria based on the source parameters.<br>To define a new destination flow, navigate to **IPCS Control Center→Device Specific Settings→Destination Flow**. Select the IPCS device name in the middle pane. Select the **Add New Flow** button in the right pane. A new page is opened (not shown) where the source flow information can be entered and submitted.<br>The list below shows the destination flows used for the compliance test. The first destination flow below (***server_client***) shows that the destination criteria will match anything, since both the **Called URI Group** and **Destination Subnet** columns contain a *****. In addition, the ***server_client*** flow has an **Action** of ***Apply Policy*** and a **Policy Group** of ***4policy_set***. Thus, the result of the ***server_client*** destination flow is to apply the ***4policy_set*** policy to all traffic from source flow 1 (**Source Subnet *10.75.5.0/24***). Similarly, the ***client_server*** destination flow will result in applying the ***3policy_set*** policy to all traffic from source flow 2 (**Source Subnet *46.16.2.0/24***).<br> |

| Order | Flow ID | Called URI Group | Destination Subnet | Action | Policy Group | Log |
|---|---|---|---|---|---|---|
| 1 | server_client | * | * | Apply Policy | 4policy_set | ☑ |
| 2 | client_server | * | * | Apply Policy | 3policy_set | ☑ |
| 3 | default | * | * | Apply Policy | default-nat | ☑ |

| Step | Description |
|---|---|
| 7. | **Policy Group (*4policy_set*)**<br>A policy group defines a set of rules that may be applied to different aspects of the destination flow.<br><br>To define a new policy group, navigate to **IPCS Control Center→Domain Policies→Policy Groups**. Select the **Add Group** button in the middle pane. A new page is opened in the right pane (not shown) where the policy group information can be entered and submitted.<br><br>The example below shows the ***4policy_set*** policy group assigned to the ***server_client*** destination flow in the previous step. The default rule is assigned to each policy category except for **Media** and **Routing**. The **Media** rule is assigned ***default-nat***. For details on the default rules, including ***default-nat,*** see [9]. The **Routing** rule, ***3routing***, is defined in the next step.<br><br> |

| Order | Time of Day | Signaling | Application | Media | Security | Routing |
|---|---|---|---|---|---|---|
| 1 | default | default | default | default-nat | default | 3routing |

| Step | Description |
|---|---|
| 8. | **Routing Rule (*3routing*)**<br>A routing rule defines how routing is performed on the destination flow.<br>To define a new routing rule, navigate to **IPCS Control Center→Domain Policies→Routing Rules**. Select the **Add Rule** button in the middle pane. A new page is opened in the right pane (not shown) where the routing rule information can be entered and submitted.<br>The example below shows the ***3routing*** rule assigned to the ***4policy_set*** policy group in the previous step and used by the ***server_client*** destination flow. This routing rule will use UDP for the transport protocol in both the incoming and outgoing directions. A server is not configured under the **Next Hop Routing** section. In this destination flow, traffic is flowing from Avaya SES to the remote endpoints. IPCS knows how to reach the endpoints from its internal database, built from monitoring the endpoint registration messages. Thus, a next hop server does not need to be configured.<br><br> IPCS Control Center<br>Sipera Systems<br>Alarms<br>Incidents<br>Statistics<br>Users<br>Logout<br>Help<br>About<br>IPCS Control Center<br>Welcome<br>Administration<br>Installation Wizard<br>Flow Wizard<br>Global Parameters<br>Domain Policies<br>Application Rules<br>Media Rules<br>Routing Rules<br>Security Rules<br>Signaling Rules<br>Time of Day Rules<br>Policy Groups<br>URI Groups<br>Device Specific Settings<br>Protected Network<br>TLS Management<br>Add Rule<br>Rename Rule<br>Clone Rule<br>Delete Rule<br>Click here to add a description.<br>Routing Configuration<br>Edit<br>Welcome ipcs, you signed in as Admin. Current server time is **12:22:07 PM EDT**<br>IPCS Control Center > Domain Policies > Routing Rules : 3routing<br>**Rules**: default, 2routing, 3routing<br>**Next Hop Routing**<br>Use DNS Resolution for SIP Server<br>☐ NAPTR ☐ SRV<br>**Transport**<br>Incoming Transport: TLS ☐ TCP ☐ UDP ☑<br>Outgoing Transport: TLS ○ TCP ○ UDP ●<br>Connection Options: ☐ Reuse Existing Connection ☐ Initiate Connection |
| 9. | **Policy Group (*3policy_set*)**<br>Repeat **Step 7** to create the ***3policy_set*** policy group shown below.<br><br> IPCS Control Center<br>Sipera Systems<br>Alarms<br>Incidents<br>Statistics<br>Users<br>Logout<br>Help<br>About<br>IPCS Control Center<br>Welcome<br>Administration<br>Installation Wizard<br>Flow Wizard<br>Global Parameters<br>Domain Policies<br>Application Rules<br>Media Rules<br>Routing Rules<br>Security Rules<br>Signaling Rules<br>Time of Day Rules<br>Add Group<br>Rename Policy Group<br>Add Policy Set<br>Delete Policy Group<br>Click here to add a description.<br>Click here to add a description.<br>Policy Set<br>Welcome ipcs, you signed in as Admin. Current server time is **12:19:27 PM EDT**<br>IPCS Control Center > Domain Policies > Policy Groups : 3policy_set<br>**Groups**: default, default-nat, 3policy_set, 4policy_set<br>Order: 1 \| Time of Day: default \| Signaling: default \| Application: default \| Media: default-nat \| Security: default \| Routing: 2routing |

| Step | Description |
|---|---|
| 10. | **Routing Rule (*2routing*)**<br>Repeat **Step 8** to create the ***2routing*** routing rule shown below and used by the ***client_server*** destination flow. In this rule, the next hop is specifically defined as the IP address of Avaya SES (***10.75.5.6***). All other values are configured the same as **Step 8**.<br><br> IPCS Control Center<br>Welcome ipcs, you signed in as Admin. Current server time is 12:20:54 PM EDT<br>Sipera Systems<br>Alarms<br>Incidents<br>Statistics<br>Users<br>Logout<br>Help<br>About<br>IPCS Control Center<br>Welcome<br>Administration<br>Installation Wizard<br>Flow Wizard<br>Global Parameters<br>Domain Policies<br>Application Rules<br>Media Rules<br>Routing Rules<br>Security Rules<br>Signaling Rules<br>Time of Day Rules<br>Policy Groups<br>URI Groups<br>Device Specific Settings<br>Protected Network<br>TLS Management<br>IPCS Control Center > Domain Policies > Routing Rules : 2routing<br>Add Rule<br>Rules<br>default<br>2routing<br>3routing<br>Rename Rule<br>Clone Rule<br>Delete Rule<br>Click here to add a description.<br>Routing Configuration<br>Edit<br>**Next Hop Routing**<br>Use This SIP Server<br>Primary IP 10.75.5.6 Secondary IP<br>**Transport**<br>Incoming Transport: TLS □ TCP □ UDP ☑<br>Outgoing Transport: TLS ○ TCP ○ UDP ●<br>Connection Options: □ Reuse Existing Connection □ Initiate Connection |

# 9. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Sipera IPCS 310 with Avaya SIP Enablement Services and Avaya Communication Manager. This section covers the general test approach and the test results.

## 9.1. General Test Approach

The general test approach was to make calls through IPCS using various codec settings and exercising common PBX features. Calls were made between the remote users and the main office, between the remote users and the PSTN, and between the remote users.

## 9.2. Test Results

IPCS passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Successful registrations of endpoints at the main and branch offices.
- Calls between a remote user without NAT and both SIP and non-SIP endpoint at the main site.
- Calls between a remote user with NAT and both SIP and non-SIP endpoint at the main site.
- Calls between a remote user with and without NAT and the PSTN.
- Calls between a remote user without NAT and a remote user with NAT.
- Calls between remote users behind the same NAT.
- Calls between remote users behind different NATs.
- G.711u and G.729AB codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.

- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.
- Extended telephony features using Avaya Communication Manager Feature Name Extensions such as Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after an IPCS restart and loss of IP connection.

The following observations were made during the compliance test:

- For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

# 10. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all remote endpoints are registered with Avaya SES using the private IP address of IPCS. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between a remote user without NAT and SIP and non-SIP endpoints at the main office.
- Verify that calls can be placed between a remote user with NAT and SIP and non-SIP endpoints at the main office.
- Verify that calls can be placed between remote users with and without NAT.

# 11. Support

For technical support on IPCS, contact Sipera support at www.sipera.com/support.

# 12. Conclusion

Sipera IPCS passed compliance testing with the observations listed in **Section 9.2**. These Application Notes describe the procedures required to configure Sipera IPCS to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support remote users with NAT traversal as shown in **Figure 1**.

# 13. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 5.0, February 2007.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.

[3] *SIP support in Avaya Communication Manager Running on the Avaya S3800, S8400, S8500 Series and S8700 Series Media Server*, Doc # 555-245-206, Issue 6.1, March 2007.

[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005

[5] *Installing and Administering SIP Enablement Services*, Doc# 03-600768, Issue 4, May 2007.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.

[7] *Concepts and Examples ScreenOS Reference Guide*, Release 5.4.0, Rev.B.

[8] *IPCS210_310 Installation Guide (230-5210-31).*

[9] *IPCS Administration Guide (010-5310-31).*

Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for Netscreen products may be found at http://www.juniper.net.

Product documentation for IPCS can be obtained from Sipera. Contact Sipera using the contact link at http://www.sipera.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.